tijdschrift van het

nederlands elektronica- en radiogenootschap

deel 56 nr. 1 1991

nederlands elektronica- en radiogenootschap

Nederlands Elektronica- en Radiogenootschap
Postbus 39, 2260 AA Leidschendam. Gironummer 94746
t.n.v. Penningmeester NERG, Leidschendam.

HET GENOOTSCHAP

De vereniging stelt zich ten doel het wetenschappelijk onderzoek op het gebied van de elektronica en de informatietransmissie en -verwerking te bevorderen en de verbreiding en toepassing van de verworven kennis te stimuleren.

Het genootschap is lid van de Convention of National Societies of Electrical Engineers of Western Europe (Eurel).

BESTUUR

LIDMAATSCHAP

Voor lidmaatschap wende men zich tot de secretaris.
Het lidmaatschap staat open voor academisch gegradueerden en hen, wier kennis of ervaring naar het oordeel van het bestuur een vruchtbaar lidmaatschap mogelijk maakt. De contributie bedraagt *f* 60,— per jaar.

Studenten aan universiteiten en hogescholen komen bij gevorderde studie in aanmerking voor een junior-lidmaatschap, waarbij 50% reductie wordt verleend op de contributie. Op aanvraag kan deze reductie ook aan anderen worden verleend.

HET TIJDSCHRIFT

Het tijdschrift verschijnt zesmaal per jaar. Opgenomen worden artikelen op het gebied van de elektronica en van de telecommunicatie.

Auteurs die publicatie van hun wetenschappelijk werk in het tijdschrift wensen, wordt verzocht in een vroeg stadium contact op te nemen met de voorzitter van de redactiecommissie.

De teksten moeten, getypt op door de redactie verstrekte tekstbladen, geheel persklaar voor de offsetdruk worden ingezonden.

De abonnementsprijs van het tijdschrift bedraagt *f* 60,—. Aan leden wordt het tijdschrift kosteloos toegestuurd.

Tarieven en verdere inlichtingen over advertenties worden op aanvrage verstrekt door de voorzitter van de redactiecommissie.

REDACTIECOMMISSIE

ONDERWIJSCOMMISSIE

IN MEMORIAM

DR. IR. KLAAS POSTHUMUS

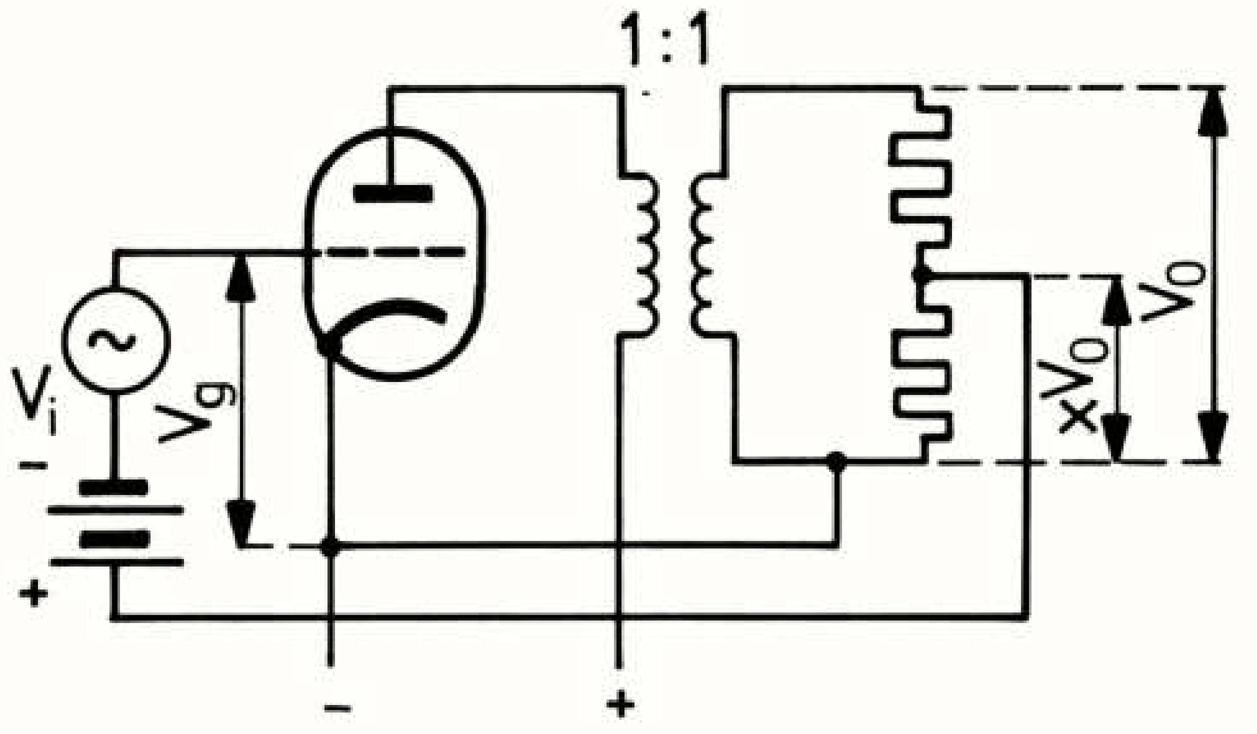
geboren te Weststellingwerf: 2 juni 1902,
overleden te Haarlem 4 oktober 1990.



Klaas Posthumus doorliep de H.B.S. in Den Haag, 1914-1919. Toen hij zijn eindexamen had afgelegd, wilden zijn ouders hem graag verder laten studeren aan de Technische Hogeschool te Delft. Dat gaf enige moeilijkheden en zijn vader ging naar de Wethouder van Onderwijs in Den Haag, om te vragen of er mogelijkheden waren, om een goede student een beurs te laten krijgen. Dat was iets nieuws voor Den Haag, maar ten slotte werd besloten, dat de gemeente Den Haag jaarlijks voor vijf talentvolle jongelui een beurs kon verstrekken. Klaas Posthumus was een van de vijf eerst uitverkorenen. Om deze studenten in het oog te houden verzocht de gemeente aan een aantal Haagse autoriteiten om de drie maanden een oog in het zeil te houden. Voor Posthumus was dit Ir. Lely befaamd door de Zuiderzeewerken. Vijftig jaar later keek Posthumus nog met voldoening terug op de "zeer waardevolle" driemaandelijkse gesprekken. In 1924 studeerde hij met lof af als elektrotechnisch ingenieur. Zijn afstudeerwerk deed hij bij Prof. Jhr. Dr. Elias. Hij solliciteerde bij Philips, waar hij ontvangen werd door Dr. G. Holst, Dr. Balth. Van der Pol en Anton Philips. De laatste nam hem officieel aan. Hij trad in dienst op 1 augustus 1924, en ging bij Van der Pol aan zendtrioden werken. Hij werd echter opgeroepen voor militaire dienst, en was ca. 5 1/2 maand in dienst, bij de genie, beginnend 1 februari 1925. Na zijn eerste opleiding kwam hij bij de radioverbindingsdienst onder kapitein Ir. Nordlohne. Deze zou hem enkele jaren later volgen naar Philips Nat. Lab. Nog voor hij uit de dienst ontslagen was, bereikte hem de mededeling, dat hij met Van der Pol bij RCA en andere radiofirma's in Amerika kon gaan kijken. Zij gingen voor zes weken naar Amerika, direct na zijn militaire dienst. Van der Pol moet wel een heel goede indruk van zijn werk gehad hebben! Behalve over triodezenders (ten gevolge van het vinden van een chroomijzerlegering met dezelfde uitzettingscoëfficiënt als glas, was de waterkoeling gemakkelijker mogelijk geworden) schreef hij ook over de labiliteit van een uit n trioden bestaande versterker (Tijdschrift N.R.G. 3, 106-112, 1927). Lange tijd hadden Oosterhuis, Bruines en Posthumus wekelijks een conferentie met mensen uit de fabriek over zendbuizen. Hij schreef ook met Groeneveld en Van der Pol over roostergelijkrichting (1927) en alleen over tetrodes in schermroosterschakeling (1928). Een andere bijdrage ging over de stroomverdeling in een eenlagige spoel met inachtname van de wederkerige inductie tussen paren spoelelementen. Hij bestudeerde ook het reflectie vrij maken van hoogfrequent leidingen.

Eind 1927 kreeg Posthumus de opdracht een meetversterker met een groot frequentiegebied en lage distorsie te bouwen. Dit leidde tot het inzicht in de tegenkoppeling, dat 19 september 1928 voerde tot een octrooischrift over "Inrichting voor het zonder vervorming versterken van elektrische trillingen". De hoofdconclusie bevatte het kenmerk, dat een x-te gedeelte van de uitgangspanning op de primaire zijde van de versterkerschakeling in tegenfase wordt teruggekoppeld. (Zie fig. 1.) Dat dit fundamentele octrooi pas in 1934 werd verleend, komt waarschijnlijk ook, omdat Black bij Bell Telephone ongeveer gelijktijdig een octrooi indiende, om tegenkoppeling toe te passen bij telefonieversterkers. Ten slotte verkregen zij beide hun octrooi.

Posthumus had ondertussen ook veel aandacht besteed aan de constructie van een kortegolfontvanger, de Philips 2802. Om klachten over ontvangers en zenders in Nederlandsch Indië na te gaan, werd besloten, dat Haverdroeze als commercieel, en Posthumus als technisch



Figuur 1. Tegenkoppeling.

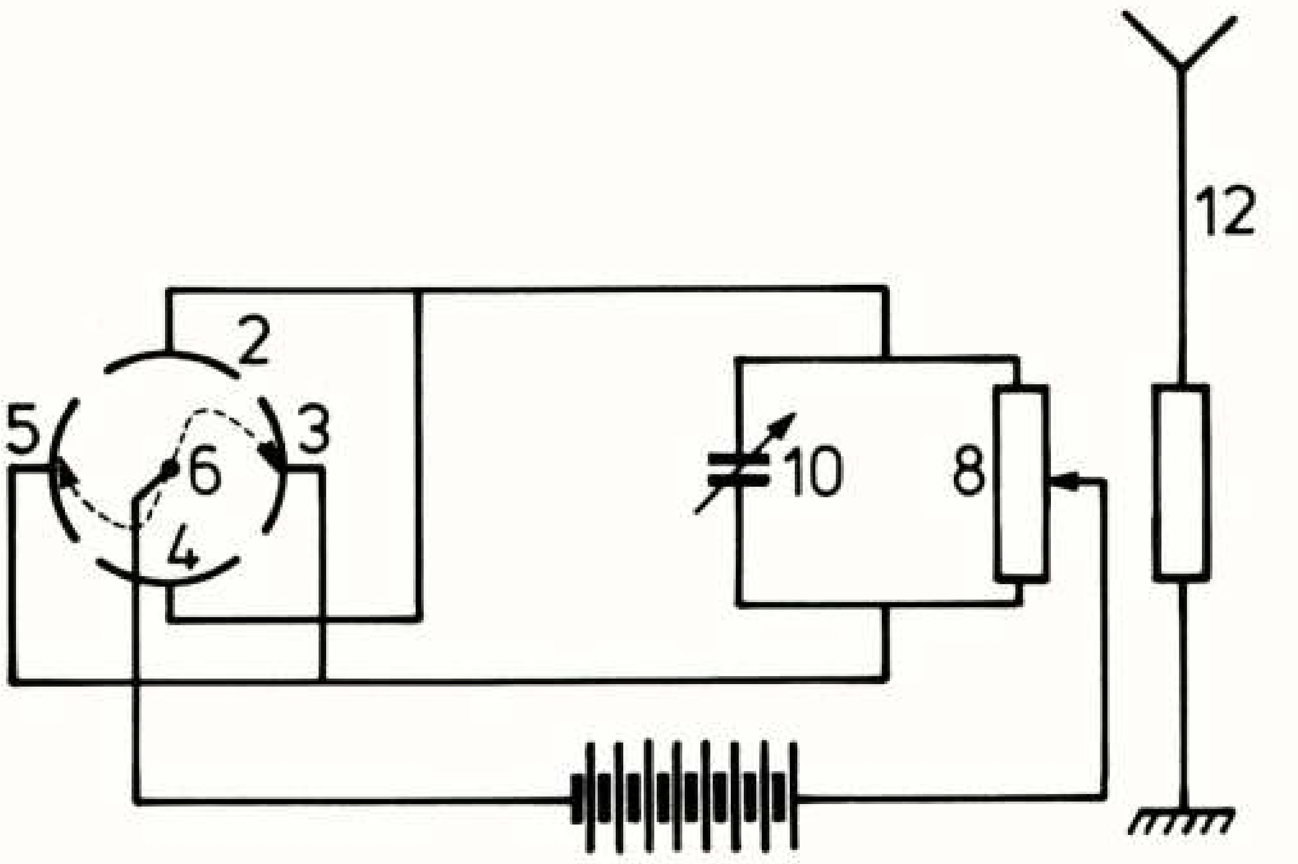
medewerker de gang van zaken ter plaatse zouden opnemen. Zij vertrokken 1 augustus 1928 per boot, en troffen aan boord ook de ingenieurs Koomans en Schotel van de Nederlandse PTT. Hoewel er enige concurrentie was tussen Philips en PTT, wat betreft de kortegolfverbinding met Indië (beide partijen zouden voor hun werk in 1929 en 1930 prijzen van het Vederfonds krijgen) was de persoonlijke verhouding goed. Posthumus en Haverdroeze werkten vanuit de Philips vestiging in Bandoeng. Ze zonden wekelijks lange telegrammen in code naar Nederland, 600 woorden à *f* 2,— per woord. Mevrouw Posthumus kreeg in oktober de eerste baby. Ze belde wel eens op, vanuit een cel in gebouw Kortenaerkade, PTT Den Haag. Later was Posthumus voor zendproblemen ook een deel van de tijd op de marinebasis Soerabaja. Na acht maanden keerden ze terug naar Nederland.

Een project, dat in dezelfde tijd speelde, en vermoedelijk door zijn assistenten in zijn afwezigheid werd voortgezet, was het simuleren van een radio-ontvanger op 500 Hz. Men wilde met behulp van een oscillograaf inschakelverschijnselen zichtbaar maken. De ouderen onder ons zullen zich de spiegeloscillograaf kamer herinneren, die door Scharp de Visser was ingericht, en die men kon reserveren, om bijv. een dag lang oscillografische proeven te doen en foto's te maken.

Tot de assistenten van Posthumus behoorden geruime tijd de heren Broos, Koffyberg, Pasma, die later in de afdelingen meetinstrumenten en radio-apparaten van de fabriek hun carrière zouden voortzetten. Ook Gehrels, Zaaijer en Douma moeten genoemd worden. (De laatste ging na het vertrek van Posthumus naar RCA, maar kwam met pensioen naar Nederland terug.) Tot de ingenieurs, die kort of langer in de groep Posthumus werkten, behoorden Alma (al rond 1929), Staal (vooral bekend door vroege radar-achtige waarnemingen aan schepen), Van de Weg (later adjunct-directeur), en Bruining.

In 1933 diende Posthumus, tezamen met Van der Pol, een octrooischrift in, dat de, zich bij automatische sterkteregeling wijzigende stuurrooster-anode capaciteit, met behulp van een weerstand in de aan stuurrooster en anodeketen gemeenschappelijke kathodeleiding compenseerde (tegenkoppeling). Dit "Posthumus weerstandje" berust in al zijn eenvoud op fundamenteel en helder inzicht in de werking van hoogvacuümbuizen in versterkerschakelingen. Een ander octrooi minimaliseert de terugwerking op de stuurrooster keten door een zo kort mogelijke verbinding tussen schermrooster en buisvoet (1934).

Ondertussen werd er ook naar gestreefd om het frequentiegebied van zenders naar hoge frequenties uit te breiden. Reeds in 1933 analyseerde Posthumus het mechanisme van een cylindrische diode met een magnetisch veld parallel aan de as. Hij vond, dat de hoogste frequentie bepaald werd door de overgangstijd van een elektron van cathode naar anode. Deze overgangstijd kon gereduceerd worden door de cylindrische anode in twee of meer paren te splitsen, waarbij tegenoverliggende sectoren binnen of buiten de buis verbonden werden, en alle tesamen met een resonantiekring. (Zie fig. 2 uit het octrooischrift.) In 1934 en 1935 verschenen een aantal fundamentele beschouwingen van Posthumus over magnetrontrillingen in "Nature" en "Wireless Engineer". Heller gaf een overzicht van dit onderzoek in Philips Technisch Tijdschrift, juli 1939. In zijn geschiedenis van de microgolfbuizen (1962) schreef Pierce, dat het werk van Posthumus een belangrijke bijdrage leverde, en een goede basis vormde voor latere meer geavanceerde theorieën over de werking van het magnetron. Wathen's "Early history of the magnetron" 1953 merkt op, dat het interactie-mechanisme tussen elektronen en de tangentiële component van een lopende golfveld, waarvan de snelheid vrijwel gelijk is aan de gemiddelde snelheid van de elektronen, door Posthumus correct geïnterpreteerd werd.



Figuur 2. Het Posthumus magnetron.

Veel magnetrons geconstrueerd volgens de principes van Posthumus werden gebruikt in een experimentele verbinding tussen Eindhoven en Tilburg, eerst op 90 en later op 25 cm. In 1935 herhaalde Posthumus zijn bezoek aan Nederlands-Indië.

In 1936 beschreef Posthumus richtantennes met identiek richtingsdiagram, maar ongelijke stroomverdeling. Voor een kortegolfcongres in Wenen, 1937, gaf hij een overzicht over kortegolfbuizen. Hij herinnerde zich later, dat bij dit congres een medicus hem aansprak over de mogelijkheid korte golven (10 cm) te gebruiken bij de bestrijding van kankergezwellen. Naar ik meen heeft ook Manfred von Ardenne deze mogelijkheid bekeken.

In 1938 begon men op het eiland Texel met experimenten over de reflectie van radiogolven door schepen. Toen in 1940 de Duitse bezetting dreigde, was het programma nog niet klaar en de ingenieurs van de regering (met Jhr.Ir. Von Weiler) gingen naar Engeland om de Britse radar research te versterken. Bij de mobilisatie van Nederland in 1938 werd Posthumus opgeroepen om dienst te doen in de radiodienst vesting Holland. Helaas bleek deze nog niet te bestaan, waarna Posthumus naar Eindhoven terugkeerde. In mei 1940 kreeg hij opnieuw een oproep, en hij voegde zich in uniform bij de Philips Nat. Lab. groep, die naar Engeland wilde. Door de vroegtijdige inzet van Duitse parachutisten kwam deze groep niet verder dan Oud-Beijerland, zodat hij ook ditmaal spoedig naar Eindhoven kon terugkeren.

In 1943 kwam Posthumus in aanraking met problemen van rijen enen en nullen (via digitale telefonie). Een P_n cyclus is een geordende reeks van 2^n digits 0 of 1, zodat de 2^n mogelijke geordende sets van n opeenvolgende digits uit die cyclus alle verschillend zijn. Een P_3 cyclus is 00010111, waarbij men zich de cyclus geplaatst denkt langs een cirkel, zodat de opvolgende drietallen zijn: 000, 001, 010, 101, 011, 111, 110, 100. Er is nog een andere P_3 cyclus 11101000. Voor P_4 cyclus zijn er 16 verschillende cycli en voor P_5 2048. Posthumus giste, dat de algemene formule voor het aantal verschillende cycli bij P_n:2 tot de macht 2^{n-1} -n zou zijn. Hij vertelde dit vermoeden aan Dr. N.G. de Bruyn, de wiskundige, die toen op het Nat. Lab. vertoefde. Deze vond eerst nog, dat de uitdrukking voor n=6 ook gold, en vervolgens het algemene bewijs, dat hij op 29 juni 1946 aan de Academie mededeelde. Later bleek, dat A. de Rivière het probleem al had voorgesteld in 1894, en dat C. Flye Saint-Marie toen de oplossing korte tijd later publiceerde. Prof.Dr.Ir. Oberman dacht dat Baudot mogelijk al eerder aan dit probleem gewerkt had.

In de oorlogsjaren ging Posthumus praktisch eens per week naar Hilversum voor technische adviezen aan de N.S.F. Het was dus geen wonder, dat hij op 1 maart 1946 overging naar de N.S.F. Zoals hij later zei, heeft het hem altijd gespeten, dat hij niet op het Natuurkundig Laboratorium was gebleven, maar de onvergetelijke Professor Holst zei altijd "Op een research laboratorium moet je jong zijn" en Holst had meestal gelijk. (Prof. Van der Pol had de overstap ontraden.) Op 1 april 1947 werd Posthumus adjunct-directeur van de Philips Telecommunicatie Industrie, en op 1 januari 1949 directeur. Dit waren de hoogtepunten van zijn loopbaan, ook al omdat P.T.I. in Hilversum en Huizen in die periode sterk gegroeid was. Men herinnert zich uit die tijd, dat het bureau van Posthumus altijd vol was met berekeningen, die hij zelf wilde doen. Zijn succesvolle en inspirerende leiding van het wetenschappelijk werk van zijn medewerkers in Eindhoven, Hilversum en Huizen werd bij zijn erepromotie uitdrukkelijk vermeld. Op 1 februari 1955 werd Posthumus wetenschappelijk adviseur van P.T.I., waarbij hij zijn directoraat niet voort kon zetten. De bedoeling was, dat hij na de jaarvergadering van 1957 wetenschappelijk adviseur van het Natuurkundig Laboratorium zou worden. Hoewel degenen, die op het Nat. Lab. in deze richting werkten, daarover geïnformeerd waren, was Posthumus zelf niet op de hoogte. Toen hij het ten slotte hoorde, wilde hij het niet meer aanvaarden. In onderling overleg heeft hij zich toen om gezondheidsredenen teruggetrokken per eind 1958. Als geheel zag Posthumus de P.T.I. periode als een anti-climax.

Na zijn pensionering vond Posthumus nog tweemaal de erkenning van de wetenschappelijke wereld. Op 17 mei 1968 ontving hij de gouden Speurwerk medaille van het Koninklijk Instituut van Ingenieurs. Prof. Dr.Ir. Oberman gaf in zijn toespraak de considerans, die door de professoren Stieltjes, Oberman, Niesten, Pelser, Roorda en Von Weiler en door Mr.Ir. De Haan was voorgesteld. Zij dachten vooral aan het speurwerk, zoals dat door octrooischriften tot uiting werd gebracht. In de oorkonde staat, dat de gouden Instituutsmedaille voor Speurwerk op de gebieden elektrotechniek en technische natuurkunde aan Ir. Klaas Posthumus is toegekend op grond van zijn uitgebreid speurwerk op het gebied van elektronische schakelingen en constructies voor de telecommunicatie, dat belangrijke resultaten ten gevolge heeft gehad. Dit speurwerk wordt gekenmerkt door een breed fundamenteel inzicht in de fysische en elektronische grondslagen van telecommunicatie-ap-

paratuur, gepaard aan ingenieursvernuft om dit inzicht in praktische resultaten om te zetten. Een deel van deze resultaten heeft verspreiding over de gehele wereld gevonden.

In januari 1970 werd door de Senaat van de Technische Hogeschool het doctoraat in de technische wetenschappen honoris causa toegekend aan Klaas Posthumus. Prof.Ir. J.W. Alexander sprak bij deze gelegenheid de considerans uit. Hij beschouwde vooral het werk aan tegenkoppeling en dat aan magnetrons als belangrijk. Bovendien legt hij in zijn werken getuigenis af van niet alleen gedegen ingenieurskunde, maar ook van een scheppende ingenieurskunst, gesproten uit het huwelijk van de theorie en de ervaring. In zijn dankwoord beschouwde Posthumus het Natuurkundig Laboratorium bij Philips als een paradijs voor jonge onderzoekers. Van der Pol's lessen in zuivere wiskunde en in de nieuwe elektronica waren voor hem bijzonder belangrijk. Zijn grote waardering voor Van der Pol heeft hij ook bij andere gelegenheden meermalen laten blijken.

F.L.H.M. Stumpers.

AUDIO ENGINEERING SOCIETY
NEDERLANDS ELEKTRONICA- EN RADIOGENOOTSCHAP
(381e werkvergadering)

UITNODIGING

voor de lezingendag op **dinsdag 25 september 1990** in het **Philips Natuurkundig Laboratorium, Prof. Holstlaan te Waalre.**

ONDERWERPEN: Digitale Audio Converters, Bit Streamer Technieken.

PROGRAMMA:

09.30 uur:	Koffie	
10.00 uur:	Aanvang programma	
12.00 uur:	Lunch (Deze lunch wordt u aangeboden door het Philips Natuurkundig Laboratorium)	
16.00 uur:	Einde programma	
Sprekers:	A. W. M. van der Enden	Grondslagen signaalbewerking
	E. C. Dijkmans	Artifacts conventionele DA-converters
	P. A. C. Nuyten	Bitstream-converter theorie
	P. J. A. Naus	Klein signaal gedrag bitstream-converters
	E. C. Dijkmans	Praktische begrenzing bitstreamer-converters

De sprekers zijn afkomstig van het Philips Natuurkundig Laboratorium

Aanmelding voor deze dag dient te geschieden vóór 19 september door middel van de aangehechte kaart **gefrankeerd** met een **postzegel van 55 cent.**
Het aantal deelnemers is beperkt, tijdstip van ontvangst van aanmelding is beslissend voor deelname.

Namens de samenwerkende verenigingen,
Kees Schouhamer Immink (AES)
040 - 74 22 21

Leusden, augustus 1990.

Beveiliging van Open Systemen

Jan Kruys, Senior Consultant

NCR Systems Engineering B.V., Nieuwegein

Deze lezing geeft een overzicht van het begrip "open systemen" en de noodzaak tot beveiliging en gaat daarbij in op enige architectuur aspecten. Tenslotte wordt een overzicht gegeven van de internationale normen op dit gebied die op het ogenblik ontwikkeld worden.

Open Systemen

Zijn veilige open systemen wel mogelijk? Zijn veiligheid en openheid niet met elkaar in tegenspraak? Om die vragen te kunnen beantwoorden moeten begrippen duidelijk zijn: "beveiliging" en "open systemen". Om met dat laatste te beginnen: het "open zijn" van een systeem wordt bepaald door de mogelijkheden die dat systeem biedt om met andere systemen informatie uit te wisselen. Mensen zijn een goed voorbeeld van zulke systemen. De informatie uitwisseling die hier plaats vindt is mogelijk doordat u en ik de zelfde taal spreken. Vooropgesteld dat ik geen al te grote fouten tegen de nederlandse grammatica maak, zult u redelijk kunnen volgen wat ik zeg. Als u de begrippen kent die ik hanteer dan kunt u ook begrijpen wat ik zeg en vindt er pas echt informatie overdracht plaats.

Informatie overdracht is dus gebonden aan het gebruik van een gemeenschappelijke syntaxis en een gemeenschappelijke semantiek. Over de te gebruiken syntaxis en semantiek kan men afspraken maken. Ik had deze voordracht in het Engels kunnen houden: in dat geval was de syntaxis anders geweest maar niet de semantiek; die hangt samen met het onderwerp. Bij open systemen is het net zo: ook die kunnen afspraken over de te voeren syntaxis en semantiek. Om een actueel voorbeeld te noemen, EDI, Electronic Data Interchange, zaken doen per computer, vereist het gebruik van berichten die aan de internationale normen voor EDI berichten voldoen. Deze normen zijn op het ogenblik in ontwikkeling.

Normen

Normen voor open systemen worden in vele nationale en internationale organizaties ontwikkeld. De grootste daarvan is de International Standards Organization (ISO). Er zijn echter ook normen die min of meer toevallig die status krijgen omdat een product een brede acceptatie krijgt. Over dit soort de facto normen zal ik het verder niet hebben, wel over de internationale normen en hoe die tot stand komen.

De genoemde ISO is een onderdeel van de UNO; het feitelijke werk wordt gedaan door vertegenwoordigers van de nationale lichamen zoals het NNI hier in Nederland. ISO normen, bijvoorbeeld voor gebruiksveiligheid, spelen veelal een rol bij afspraken over handel tussen landen.

Een tweede belangrijke organisatie is de CCITT, het Committee Consultative International de la Telegraphie et de la Telephonie, een samenwerkingsverband van alle PTTs en andere informatietransporteurs ter wereld. De CCITT ontwikkelt aanbevelingen voor de aankoop van apparatuur door zijn leden en gezien de enorme markt die de CCITT vertegenwoordigt, zal het duidelijk zijn dat die aanbevelingen veel gewicht in de schaal leggen. Een derde organisatie is ECMA, de European Computer Manufacturers Association waarin alle belangrijke leveranciers - inclusief amerikaaanse en japanse - zitting hebben. ECMA maakt normen die veelal als voorzetje dienen naar ISO normen: het ECMA werk vindt men soms letterlijk terug in latere ISO normen.

Bovengenoemde organisaties ontwikkelen wat men noemt basis normen: normen die vastleggen wat een systeemontwerper zou kunnen gebruiken in zijn ontwerp. De mate van flexibiliteit die de basis normen bieden maakt het in feite erg moeilijk om open systemen tot in detail te specificeren zodanig dat het werkt met een ander open systeem. Daarom zijn er organisaties zoals EWOS, de European Workshop for Open Systems - een door de EEG gesponsorde organisatie - die zich bezighoudt met het ontwerpen van profielnormen. Een profielnorm maakt een keuze uit het repertoire van mogelijkheden dat door de basisnormen geboden wordt; zo'n keuze is dikwijls specifiek voor een bepaald toepassingsgebied.

Een andere belanrijke organisatie is de IEEE: al 100 jaar lang publiceert zij normen op het gebied van electrische systemen en van informatieverwerking. Een laatste organisatie die ik noemen wil is het Directoraat General XIII van de Europese Commissie. Recentelijk heeft deze een conceptnorm geplubliceerd voor de evaluatie en certificatie van beveiligde informatiesystemen: de Information Technology Security Evaluation Criteria. Zoals te done gebruikelijk wordt ook deze mondvol afgekort: ITSEC. Dit document zal op langere termijn zeker een rol spelen voor zewel de gebruikers als voor de leveranciers op het gebied van systeembeveiliging en produktstrategie.

Communicatie

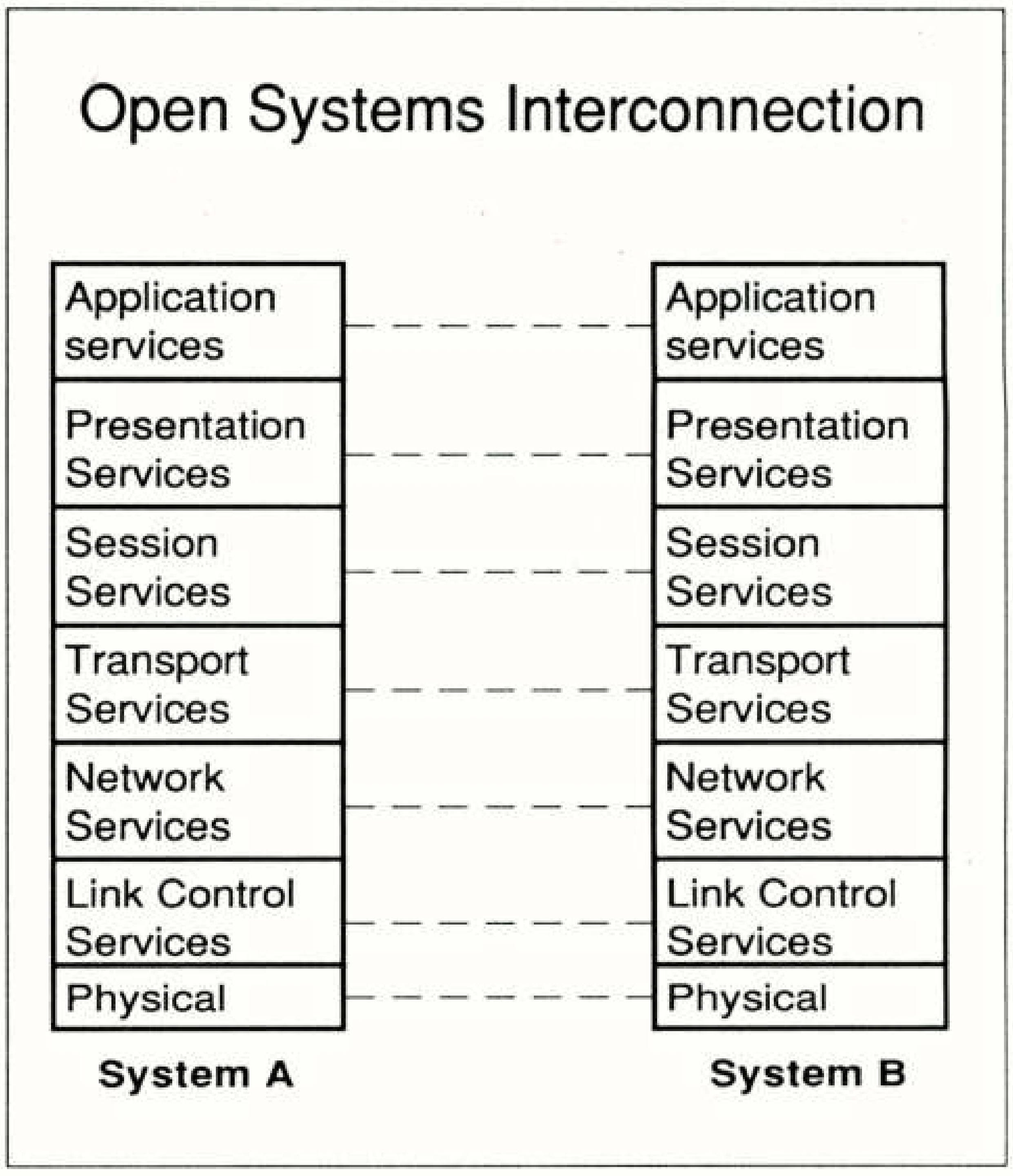
Interactie tussen open systemen vereist data communicatie, op zich een complex proces waarvoor reeds een aantal normen bestaan. Vele van deze normen zullen aangepast moeten worden ter ondersteuning van beveiligingsfuncties. Het meest gebruikte architectuurmodel voor data communicatie is het Open Systems Interconnection Reference Model (ISO 7498) dat data communicatie functies beschrijft in termen van een zevenlaags model. Zie Figuur 1. Dit model houdt zich alleen bezig met syntaxtische aspecten: de semantiek is specifiek voor een bepaalde toepassing en valt buiten het model.

Elke laag maakt gebruik van een protocol voor de synchronisatie met de corresponderende laag in het andere systeem. Als aan dit model beveiligingsfuncties worden toegevoegd dan worden die zichtbaar in uitbreidingen van de protocollen.

De hoogste laag helpt een applikatieprogramma met het opzetten van een verbinding met een andere applikatie. Netwerkaddressen en zo zijn hier onbekend: applikatienamen en -profielen (die beschrijven wat een applikatie in feite kan) zijn de parameters waarmee in deze laag gewerkt wordt. In de laag daaronder vindt omzetting plaats tussen verschillende vormen van data representatie. Bijvoorbeeld: computers hebben soms verschillende manieren om een 32 bits floating point waarde in bits uit te drukken. Ook zal applikatie programmatuur informatie volgens bepaalde conventies formatteren en het is niet waarschijnlijk dat twee willekeurig gekozen applikaties elkaar zouden "verstaan".

Laag zes vangt dit soort verschillen op door alles naar een vaste syntax te vertalen. Deze staat bekend als Abstract Syntax Notation 1 (ASN1). De Sessie laag regelt de stroom van informatie: wanneer wie mag spreken en naar welk punt in het voorafgaande men teruggaat in geval van een misverstand. De Transport laag zorgt voor het opbreken van grotere berichten in kleinere en voor multiplexing van meerdere applikatie sessies over een zelfde transport verbinding. De Netwerklaag zorgt voor het vervoer binnen het netwerk en zorgt ervoor dat de Transportlaag niets ziet van het onderliggende netwerk en de verbindingen waaruit dat netwerk is opgebouwd. Die verbindingen worden geleverd door de tweede laag die alle functies bevat voor het overbrengen van informatie tussen twee punten van een netwerk, onder andere het herhalen van berichten bij transmissiefouten. De Fysieke laag levert transmissie op bit niveau, bijvoorbeeld met behulp van modems.

Iedere laag heeft een eigen syntax en semantiek om met zijn tegenhager te kunnen communiceren en het communicatieproces op gang te houden. Op iedere laag spelen beveiligingsoverwegingen een rol.



Figuur 1

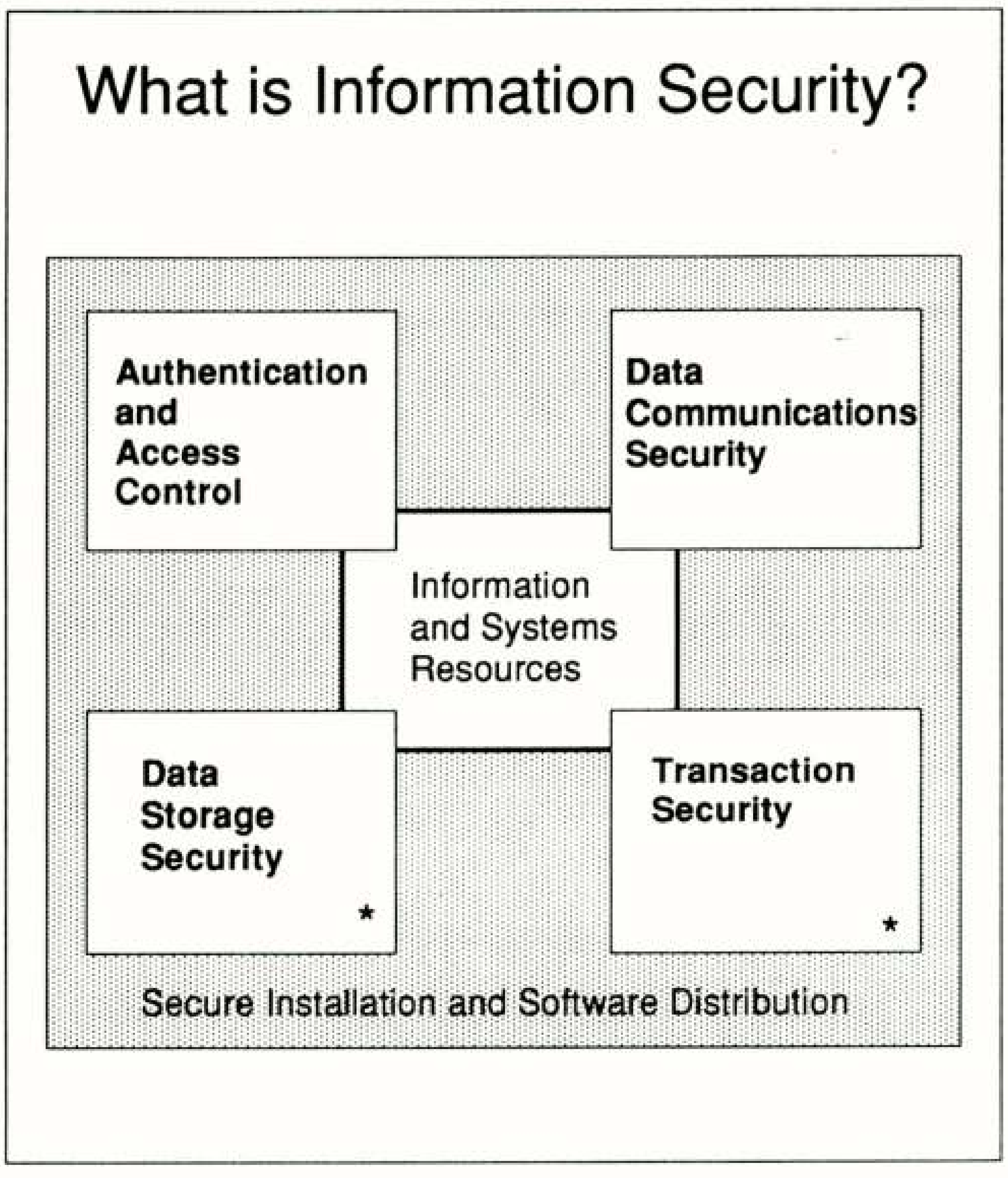
Veilige Systemen

Een **veilig systeem** is een systeem dat de daarin behandelde en opgeslagen informatie beschermt tegen misbruik en verminking. die bescherming moet gelijkelijk van toepassing zijn op alle hoofdonderdelen van het systeem: applikatie programmatuur, communicatie faciliteiten en massa opslag (e.g. op schijven) moeten beveiligd worden. Ook het operating system, dat de andere componenten beveiligd, moet zelf beveiligd worden zodat men er op vertrouwen kan. Een **veilig open systeem** is een systeem waarvan de beveiligings functies voldoen aan open systeem normen.

Een veilig open systeem is meer dan een doos waarin informatie veilig opgeborgen kan worden. Tegenwoordig zijn computers onderling verbonden door netwerken en het uitvoeren van vele functies vereist samenwerking tussen twee of meerdere computers. Die samenwerking vereist communicatie van verschillende vormen en net als de computers zelf moet die communicatie ook beveiligd worden. Daarvoor zijn normen nodig die specificeren hoe beveiligingsinformatie er uit ziet en hoe en wanneer die informatie uitgewisseld wordt.

Door na te gaan wat er met informatie gebeurt kan het brede gebied van informatiebeveiliging onderverdeeld worden in een aantal deelgebieden, zie Figuur 2. Deze onderverdeling geldt zowel voor militaire als commerciele systemen.

Zonder gegevensopslag zijn computers eigenlijk niet bruikbaar. Bovendien kan de waarde van die gegevens hoog zijn; het kan ook zijn dat verminking van die gegevens leidt tot schade. Als een diagnose, opgeslagen



Figuur 2

in een ziekenhuiscomputer, foutief is dan kunnen de gevolgen niet te overzien zijn. Er is dus behoefte aan dataopslag beveiliging.

Communicatie tussen computers maakt het mogelijk dat gegevens buiten de veiligheid van een gesloten systeem komen. Daarmee wordt het mogelijk dat die gegevens ofwel ongewild in verkeerde handen komen of, al dan niet opzettelijk, verminkt worden. Er is dus behoefte aan data communicatie beveiliging.

Veel data communicatie tussen bedrijven onderling en met andere organisaties vindt plaats in de vorm van transacties waarbij het om grote hoeveelheden geld of andere waarden gaat. Er is dus duidelijk behoefte aan transactiebeveiliging. Daar maken we allemaal gebruik van als we geld opnemen uit een geldautomaat: de PIN code die we daarbij gebruiken wordt heel zorgvuldig beschermd tegen duplicatie en ander misbruik.

Ook al is een computersysteem perfect beveiligd op bovenstaande gebieden, het blijft noodzakelijk om te controlen wie er toegang heeft tot een systeem en het blijft noodzakelijk om mensen te beperken in wat zij kunnen doen met het systeem. Er is dus ook behoefte aan authenticatie van gebruikers en aan toegangscontrole.

Welke vorm en mate van beveiliging er ook gekozen wordt, het is noodzakelijk dat de apparatuur en de programmatuur voor het systeem zelf en voor die beveiligingsfuncties betrouwbaar zijn; dit vereist een beveiliging van installatieprocedures en van programmadistributie in een netwerk.

De behoefte aan beveiliging verschilt per bedrijfstak en per bedrijf. Een bank bijvoorbeeld moet klantengegevens geheim kunnen houden maar moet er ook voor zorgen dat de boekhouding perfect klopt en niet door iedere klerk veranderd kan worden. Een groot bedrijf met weinig sociale controle zal meer behoefte hebben aan beveiliging dan een klein bedrijf waar men elkaar goed kent. Maar er zijn ook bedrijven waar perceptie door de klant een grote rol speelt en waar men daarom alleen al bereid is tot forse investeringen in informatiebeveiliging.

<u>Uitdaging</u>

De uitdaging waarvoor de computerindustrie zich gesteld ziet is het ontwikkelen - samen met gebruikers - van normen voor het beveiligen van open systemen. Die beveiliging moet flexibel zijn en effectief, gemakkelijk in het gebruik en aanpasbaar aan de eisen van de individuele organisatie. Een probleem hierbij is dat de bestaande modellen van systeembeveiliging veelal gebaseerd zijn op nu ouderwetse, gecentraliseerde systeemmodel: de grote computer met een paar duizend beeldschermen er op aangesloten.

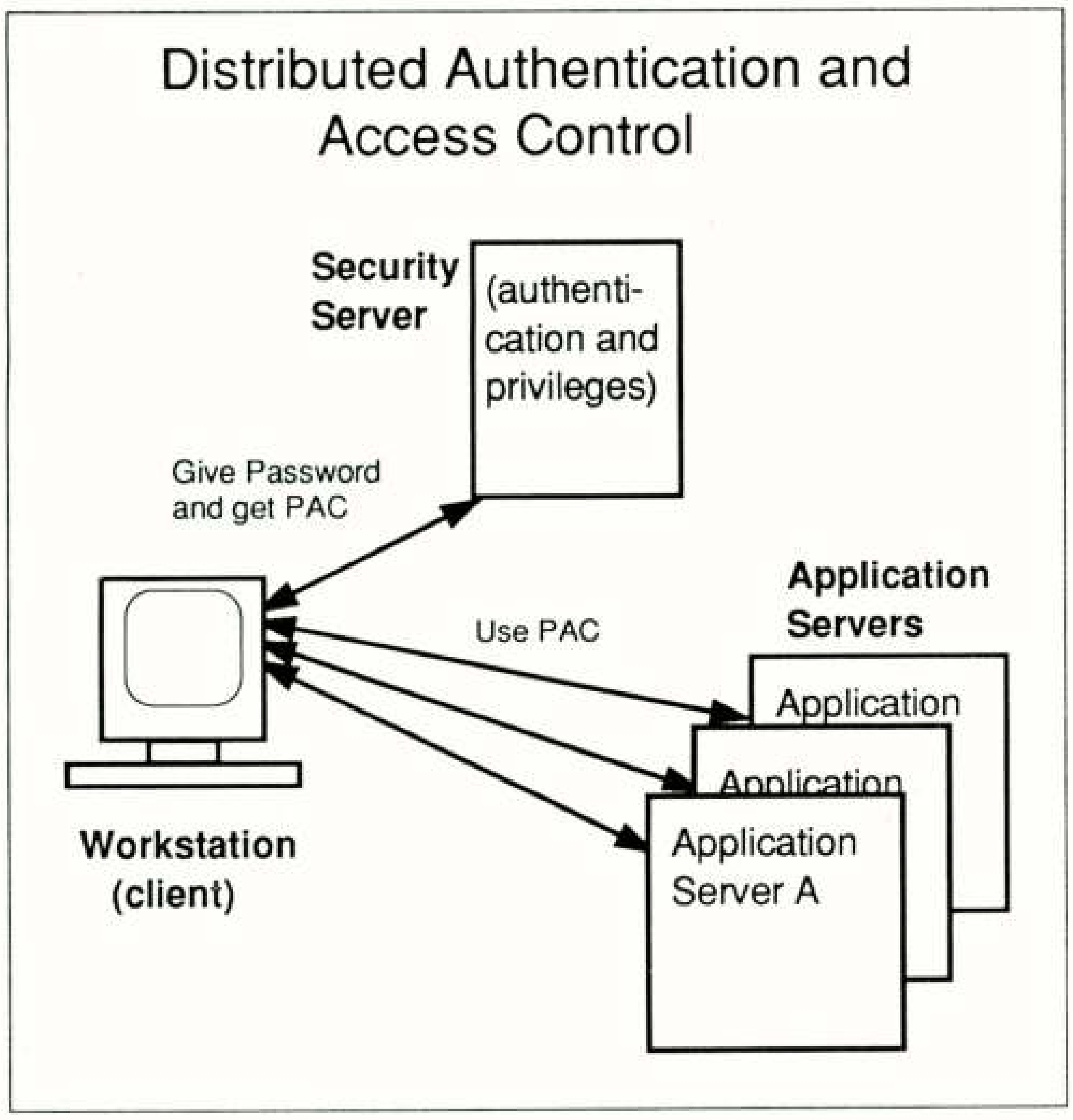
De netwerken van vandaag en meer nog die van morgen bestaan uit vele op elkaar aangesloten computers, van PCs tot grote mainframes. Applikaties en databases worden verspreid over bedrijfsnetwerken en veel zaken doen tussen bedrijven onderling zoals prijsopgave vragen, onderdelen bestellen en betalingen gebeurt nu per computer.

In dergelijke netwerken gaan de oude modellen van gegevensbeveiliging niet meer op en moeten er nieuwe modellen en nieuwe normen ontwikkeld worden.

<u>Authenticatie</u>

Een essentiele beveiligingsfunctie is het authenticeren van gebruikers: alleen gebruikers die men kent en die men toestemming gegeven heeft mogen toegang krijgen tot een systeem of netwerk. Elk van die bekende gebruikers heeft bepaalde toegangsrechten die samenhangen met de functie van die gebruiker binnen de organisatie en het vertrouwen dat die persoon geniet. Door te controleren wie toegang krijgt tot het systeem is het mogelijk bij te houden wie wat doet; iedere gebruiker kan daarmee gecontroleerd worden en kan ter verantwoording worden geroepen als er fouten gemaakt worden.

Authenticatie levert de basis voor al deze functies. Er zijn vele manieren van authenticatie. De PIN code die u gebruikt voor de geldautomaat en de toegangskode die u intikt op uw Unix systeem zijn er voorbeelden van. De laatste tijd komen de zogenaamde smart cards in zwang, vooral bij banken. De kaarten bevatten een micro computer waarin onder andere authenticatie informatie kan worden opgeslagen. Meneer



Figuur 3

Goudriaan gaat u daarover straks meer vertellen. Retina-aftasting en vingerpatroon-herkening worden meer gebruikt voor systemen waar veiligheidseisen een belangrijkere rol spelen dan kosten.

In een netwerk kan het nodig zijn dat gegevens die voor authenticatie gebruikt worden - de PIN kode bijvoorbeeld - op veilige wijze overgebracht kan worden van de ene computer naar de andere.

Toegangscontrole

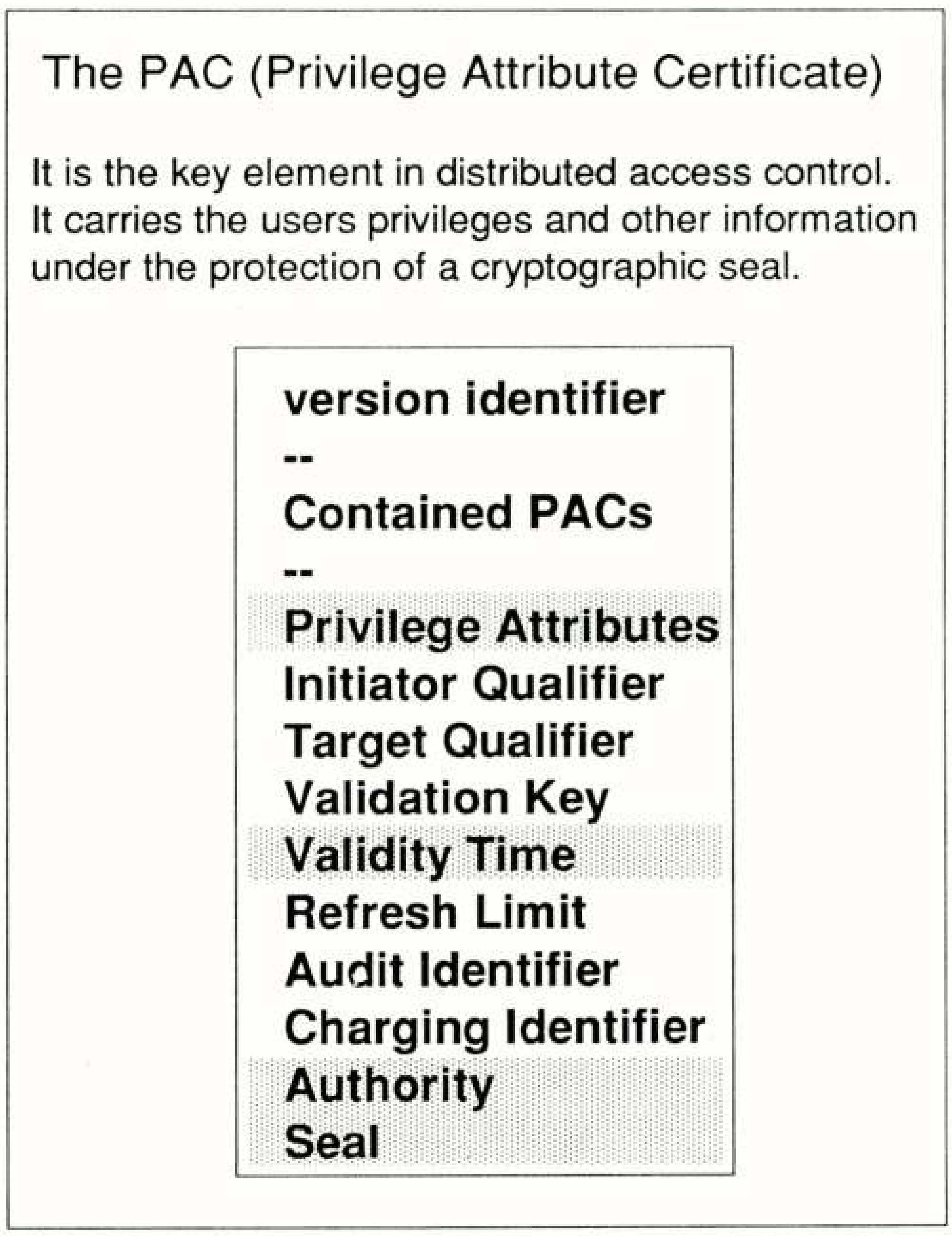
Toeganscontrole is een zaak van het toekennen ven privileges aan gebruikers en het is een zaak van het vaststellen van welke controles er toegepast worden bij het toegang geven tot een bepaald programma of gegevensbestand. De privileges fungeren als sleutels die in de sloten, de controles van objecten passen. Privileges kunnen zeer specifiek zijn en kunnen gebruikt worden om bepaalde gebruikers specifieke dingen te laten doen. Bijvoorbeeld: Meneer A. kan financiele transacties doen tot een bedrag van 6000.- gulden maar meneer B. mag tot 12000.- gulden gaan. Afhankelijk van de organisatie en de manier waarop zij werkt kunnen privileges en controles algemeen zijn (bijvoorbeeld "gasten kunnen alleen bestanden lezen op disc C") tot zeer specifiek (bijvoorbeeld Meneer Y mag met programma A de gegevens in bestand X veranderen). Dit laatste voorbeeld is gebaseerd op een nieuw beveiligingsmodel dat in 1988 door de Amerikanen Clark en Wilson werd voorgesteld.

In conventionele systemen wordt toegangscontrole veelal uitgevoerd door een deel van het operating system, de kernel, die alle interactie van programmatuur en bestanden beheert. In een multi-user systeem (zoals Unix bijvoorbeeld) kent zo'n kernel alle gebruikers, alle applikaties en alle bestanden en hij kan dus heel goed toegangscontrole uitoefenen.

In een netwerksysteem wordt dat wat moeilijk: de kernel van elk netwerkknoop kent z'n eigen gebruikers, bestanden, enz maar niet die van andere computers. Om een proces in computer A met een object in computer B te laten werken moeten de kernels van die twee computers dus samenwerken, zij moeten van elkaar begrijpen hoe privileges gespecificeerd worden en hoe die zich verhouden tot de controles van bestanden en andere objecten.

Nu is samenwerking tussen twee systemen nog wel te regelen maar als het veel systemen worden in een groot netwerk dan wordt het echt moeilijk: het aantal relaties tussen de netwerkknopen is gelijk aan het aantal verbindingen en dat aantal loopt op met het kwadraat van het aantal knopen. Het is daarom beter met een "derde partij" te werken, met een "security server" die door alle andere systemen vertrouwd wordt en die alle authenticatie en privilegetoewijzingen voor zijn rekening neemt. Zie Figuur 3. Dat kan allemaal als die security server en de andere netwerk componenten elkaar begrijpen. Er is zijn dus normen nodig die beveiligings- protocollen specificeren, syntax vastleggen en die de semantiek van privileges en controles die worden uitgegeven door zo'n security server, definieren.

Aan deze normen wordt nu gewerkt in ECMA en in de ISO. De eerste norm op dit gebied was ECMA Standaard 138,



Figuur 4

beter bekend bij de informele werknaam "Alice in Wonderland". Deze norm definieert een syntax voor het uitwisselen van privileges in een open netwerk. De kern van deze syntax is een cryptografisch beveiligd certificaat dat een aantal vaste en aantal optionele parameters bevat, allemaal gespecificeerd in ASN1, de abstracte syntax van de ISO. Zie Figuur 4. De vaste kern wordt gevormd door toepassings-specifieke privileges, de geldigheidsduur en de uitgifteinstantie. Die laatste is ook degene die de cryptografische beveiliging aanbrengt op het certificaat. Ieder systeem dat zo'n Privilege Attribute Certificate (PAC) ontvangt kan beslissen of het de uitgever ervan erkent en of de privileges voldoende zijn voor wat de gebruiker op dat moment wil. De ECMA norm definieert nog een aantal andere attributen van de PAC zoals bijvoorbeeld de Initiator en Target Control Attributes. Deze maken het mogelijk dat de uitgever precies kan specificeren voor welke gebruiker en voor welke objecten de PAC geldig is. Met zorg zijn deze optionele parameters zo gekozen dat een groot aantal manieren van beveiliging ook uitgevooerd kan worden met behulp van deze PACs. ECMA 138 is wat men noemt "security policy independent".

Data Communicatie Beveiliging

De beveiliging van data communicatie is een ander gebied; het heeft wel enige wisselwerking heeft met bovenstaande maar is er toch in grote mate onafhankelijk van. Er is behoefte aan een aantal diensten waarvan communicatiefaciliteiten gebruik van kunnen maken. Het OSI Reference Model (ISO 7498/2) definieert een aantal van die diensten en het geeft aan in welke lagen van het model deze diensten beschikbaar gemaakt **kunnen** worden. Deze diensten moeten het volgende bieden: confidentialiteit van berichten of delen van berichten, integriteit van berichten of delen van berichten, authenticatie van origine van berichten en non-repudiatie van berichten (bescherming tegen loochening van verzenden of ontvangen). Straks zal ik daar iets verder op ingaan.

Normering

Na dit korte overzicht van toegangscontrole en data communicatie beveiliging nu een overzicht van de activiteiten van de verschillende standardisatielichamen die op dit gebied werkzaam zijn en de onderwerpen waarmee zij bezig zijn. De laatsten vallen in vijf deelgebieden uiteen:

- Architectuur, raamwerken en modellen,
- Diensten en protocol specificaties,
- Technieken en mechanismen voor beveiliging,
- Beveiliging van gedistribueerde applikaties,
- Beheer van beveiliging.

Figuur 5 geeft een overzicht van de voornaamste organisaties en groepen die op bovengenoemde deelgebieden werkzaam zijn.

The International Groups

ISO/IEC/JTC1	SC6 : OSI Security SC14: EDI Security SC17: Smart Card Security SC18: Office Systems Security SC21: Security Architecture SC22: Operating Systems Security SC27: Techniques and Mechanisms
ISO/TC46	Information Systems Security
ISO/TC65	Safety Critical Security
ISO/TC68	Banking Security
ISO/TC154	EDI Security
CCITT	X.400, X.500, Distributed Applications Security, Telematics Security
ECMA	Open Systems Security

Figuur 5

Raamwerken

De raamwerken waaraan ISO en de CCITT werken beschrijven deelgebieden van beveiliging (authenticatie, toegangscontrole, confidentialiteit, integriteit, non-repudiatie en beveiligings audit) in detail, zij geven aan welke mechanismen en technieken van toepassing zijn, welke verbanden er zijn met andere deelgebieden, etc. De raamwerken dienen als basis voor specifieke architecturen voor beveiliging van bijvoorbeeld communicatie of databases. Op het ogenblik zijn het Authentication Framework en het Access Control Framework in ISO redelijk ver gevoorderd, de eerste is al een "draft proposal" en de tweede wordt dat volgend jaar. Als u een compact overzicht zoekt van alle deelgebieden dan kan ik u verwijzen naar ECMA Technical Report 46: Security in Open Systems, Security Framework.

Beveiliging in het OSI Model

In het geval van OSI was de beveiligings architectuur er eerst; later, op aandringen van onder andere ECMA, werden de Frameworks ontwikkeld. De OSI Security Architecture definieert een aantal beveiligingsfuncties en hun plaatsing in het zevenlaags model. Zie Figuur 6. De bovenste laag in die figuur, de applikatie laag bevindt zich eigenlijk buiten het model; deze bevat beveilingsfuncties zoals authenticatie van menselijke gebruikers, toegangscontrole, en transactie beveiliging. In de applikatie diensten laag, de bovenste laag van het eigenlijke model, gebeurt authenticatie van applikaties

Security and the OSI Model

(SC21 & SC6)

Operating Systems & Applications	Human user User Authentication, Access Control, Transaction Security
Application Services	Appl. Authentication,Access Control, Encryption, Sign's
Presentation Services	Data Encryption
Session Services	
Transport Services	Data Encryption and Sign's, System Access Control
Network Services	Data Encryption and Sign's, System Access Control
Link Control Services	Data Encryption
Physical	Data Encryption

Figuur 6

onderling, toegangscontrole tussen applikaties en data encryptie en data verzegeling door middel van elektronische handtekeningen. Laag 6 doet data encryptie - tegelijk met de omzetting naar de abstracte syntax.

De Transportlaag en de Netwerklaag doen eveneens encryptie en verzegeling op berichtniveau, onafhankelijk van en onzichtbaar voor de hogere lagen. Daarnaast staat de architectuur toe dat toegangscontrole in de Transportlaag plaats vindt. Toegangscontrole is hier beperkt tot controleren dat de applikatie die een verbinding opent, inderdaad gerechtigd is dat te doen. Met eigenlijke toegang tot gegevens heeft dit niets te maken.

Tenslotte staat de architectuur toe dat data encryptie toegepast wordt in de onderste twee lagen. Wat in de praktijk gerealiseerd wordt is een kwestie van kiezen uit de vele opties die de architectuur - een basis norm - toestaat. Regeringsinstanties in een aantal landen waaronder de VS, Engeland en Nederland hebben richtlijnen, profielen (GOSIP, Government OSI Profiles) uitgegeven voor de functies van OSI systemen, die voor regenringsinstanties aangeschaft worden. Een GOSIP document specificeert ook welke beveiligingsfuncties in welke lagen voorhanden moeten zijn. In de VS wordt bijvoorbeeld data encryptie in zowel laag 3 als laag 4 geeist. In Europa zal EWOS equivalente documenten maken voor de civiele sector, in de VS is dat het National Institute of Standards and Technology (NIST).

IEEE 802.10

Het OSI Referentie Model is niet van gisteren, het is al wat ouder, van het eind van de jaren zeventig, van voor de LAN revolutie. Local Area Networks gedragen zich meer als radionetwerken dan als kabelnetwerken en dat verschil leidt tot andere beveiligings eisen en -mogelijkheden. De IEEE heeft zich sterk gemaakt voor een alternative visie waarin laag 2 niet alleen diensten levert voor confidentialiteit maar ook voor integriteitsbewaking en voor toegangscontrole. De commissie IEEE 802.10 is bezig een norm te ontwikkelen die een tussenlaag definieert boven laag 2 en onder laag 3. Het staat nog te bezien of ISO deze norm over zal nemen. De bescherming die SILS, zoals de IEEE norm wordt afgekort, biedt is tamelijk grof van structuur en beperkt zich eigenlijk tot data stromen tussen dozen. Het is mijns inziens zeer de vraag of SILS wel relevant is voor commerciele systemen waar beveiligingseisen veelal applikatie afhankelijk zijn.

Specifieke Toepassingen

Binnen de ISO is reeds een aantal normen gemaakt of in ontwikkeling voor applikaties zoals Electronic Mail, Directories, Office applications (Document Filing and Retrieval, Printing) en Electronic Data Interchange. Elk van die normen bevat uitspraken over beveiligingsdiensten of mechanismen. De ISO SC18 normen voor Document Filing and Retrieval en voor Printing specificeren het gebruik van PACs als gedefinieerd in ECMA 138. De ISO SC21 Directory norm (ook bekend als CCITT X.500) definieert een eigen certificaat dat voornamelijk dient als drager voor cryptografische sleutels en de Electronic Mail norm (ook bekend als CCITT X.400) definiert een eigen set van beveiligingen die specifiek zijn voor een post systeem.

Veilig Bankieren

De bankwereld weet van wanten op het gebied van beveiliging. Lang voor dat ISO SC21 zich bezig ging houden met beveiliging binnen de OSI architectuur waren de specialisten van de banken in ISO TC68 al bezig met normen voor het gebruik van cryptografie voor het beschermen van transacties en met normen voor sleutelbeheer in commerciele bankdiensten. Later zijn daar normen voor PIN beveiliging, bericht encryptie, veilig aanloggen, en voor sleutelbeheer in prive bankdiensten bijgekomen.

Technieken en Mechanismen

In ISO SC27 (recentelijk verrezen uit de as van SC20) wordt gewerkt aan technieken en mechanismen voor beveiliging. Voorbeelden hiervan zijn cryptografies algoritmen, hash functies, digitale handtekeningen, authenticatie protocollen, enzovoort, dingen waar meneer Boly vanmorgen iets over verteld heeft. De normen die

SC27 maakt worden gerefereerd in andere normen, bijvoorbeeld voor sleutelbeheer.

De Toekomst

Hoewel er een grote hoeveelheid werk gedaan is en aan de gang is, er zijn nog veel normen die geschreven moeten worden. Een voorbeeld hiervan is een norm die, met de ECMA 138 norm als basis, een complete set van protocollen en koppelingen beschrijft voor een gedistribueerd veilig systeem. ECMA is aan zo'n norm bezig: "Through the Looking Glass" is de werknaam. Andere voorbeelden zijn database-beveiliging, certificatie van beveiligde systemen, richtlijnen voor het gebruik van zulke systemen, enzovoort. Er is dus werk genoeg aan de winkel. Er is zoveel werk aan de winkel dat er een tekort is aan mensen die er actief aan mee werken. En dat is jammer want de kwaliteit van de internationale normen is afhankelijk van de mensen die er aan werken. Met goede normen is iedereen gebaat, ook uw werkgever.
Mocht u kennis van zaken hebben of willen bijdragen aan het normeringswerk, stelt u zich dan in verbinding met het NNI. Of met de IEEE. Ik dank u.

ECMA Documentatie

De genoemde ECMA documenten kunt u kostenloos verkrijgen op onderstaand adres:

ECMA
114 Rue du Rhone
CH-1024 Geneve, Zwitserland
Tel: + 41 22 735 36 34

Voordracht gehouden tijdens de 382e werkvergadering.

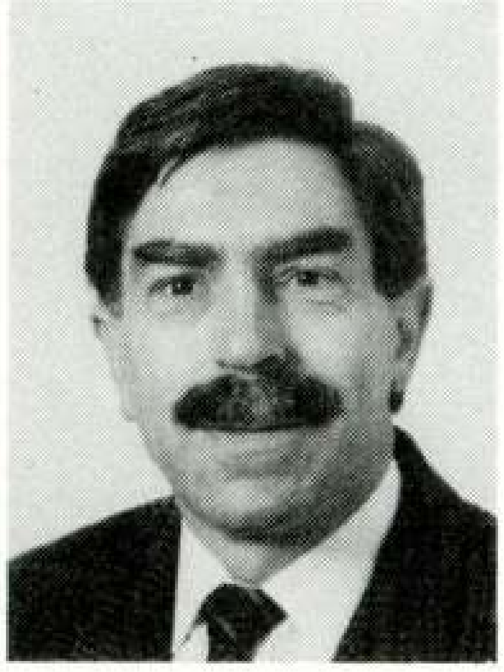
(382e werkvergadering)

THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS
BENELUX SECTION
NEDERLANDS ELEKTRONICA- EN RADIOGENOOTSCHAP
KONINKLIJK INSTITUUT VAN INGENIEURS
AFDELING TELECOMMUNICATIE

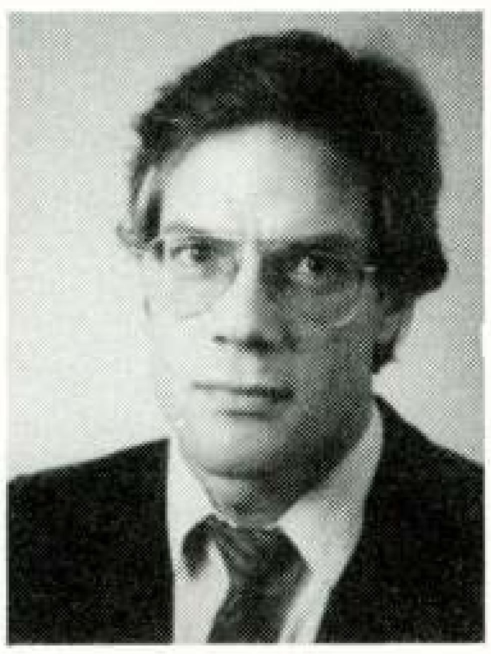
UITNODIGING

voor de lezingendag op **donderdag 18 oktober 1990** in de gehoorzaal van het PTT Research Neher Laboratorium, St. Paulusstraat 4 te Leidschendam.

THEMA: Systeem en Gegevens Beveiliging



Prof.dr.ir. D.E. Boekee



Ir. R.E. Goudriaan

PROGRAMMA:

9.30 - 10.00 uur	Ontvangst, koffie + thee
10.00 - 10.45 uur	**Ir. J.-P. Boly** (PTT Research) "Cryptologie"
10.45 - 11.15 uur	koffie + thee
11.15 - 12.00 uur	**J.P. Kruys** (NCR Systems Engineering B.V.) "Beveiliging in open systemen"
12.00 - 12.45 uur	**Prof.dr.ir. D.E. Boekee** (Technische Universiteit Delft) "Het toetsen van methoden voor sleutelbeheer m.b.v. een expert systeem"
12.45 - 14.00 uur	Lunch
14.00 - 14.45 uur	**Ir. R.E. Goudriaan** (NMB Postbank Groep) "Identificatie en chipkaarten"
14.45 - 15.15 uur	thee + koffie
15.15 - 16.00 uur	**Dr.ir. C.J.A. Jansen** (Philips Crypto B.V.) "Een sleutelbeheer systeem gebaseerd op het gebruik van smart cards"

Aanmelding voor de lezingendag dient te geschieden **vóór 1 oktober** door inzending van de aangehechte kaart gefrankeerd met 55 cent. De kosten van deelname bedragen *f* 25,—. Dit bedrag dient **vóór 1 oktober** ontvangen te zijn op postrekening 3099125 t.n.v. Penningmeester IEEE Benelux Section, Gen. v. Portlandlaan 39, 5623 KZ Eindhoven, onder vermelding van "beveiliging".
De deelname is beperkt tot leden van de drie bovenvermelde verenigingen en tot maximaal 100 personen. Alleen aanmeldingen die geschieden d.m.v. een volledig ingevulde aanmeldingskaart en tijdige betaling van *f* 25,— deelnamekosten kunnen in behandeling worden genomen. Aanname geschiedt in volgorde van binnenkomst. **Deelnemers krijgen een schriftelijke bevestiging, die zij dienen te tonen aan de ingang van het RNL.** Niet-deelnemers krijgen een schriftelijke afwijzing en krijgen hun deelnamekosten teruggestort. Deelnemers die per auto komen worden verzocht deze te parkeren bij winkelcentrum Leidsenhage (± 3 min. lopen naar het RNL) i.v.m. beperkte parkeergelegenheid op het RNL terrein.

Eindhoven, juli 1990.

Dr.Ir. W.J. van Gils,
programma coördinator IEEE Benelux Section,
tel. 040-744707

IDENTIFIKATIE EN CHIPKAARTEN

Ir R.E. Goudriaan
NMB Postbank Groep

Identification and Chipcards. A general introduction to the use of Chipcards as a means of authentication. In a society where Electronic Data Interchange is going to play a dominant role, visual methods for authentication of persons like signature verification are no longer adequate. Instead, methods for automated authentication of persons and messages are needed. One such method is based on Chipcards (integrated circuit cards). The security potential of memory chipcards and of processor chipcards will be highlighted. If the prover has a processor chipcard, it can be used as an intelligent token that can dynamically calculate a cryptographic response to the challenge posed by a verifying party. Reference is being made to existing applications and to relevant ISO standards.

Algemeen

Identifikatie van een persoon wordt tot nu toe vrijwel uitsluitend gedaan door controle op de echtheid van een papieren identifikatiebewijs, al dan niet aangevuld met vergelijking van de handtekening op dat bewijs met een ter plaatse gezette handtekening.

Visuele Echtheids- en Handtekeningcontroles worden steeds moeilijker te realiseren in geautomatiseerde omgevingen, zodat gezocht wordt naar nieuwe methoden van identifikatie waarbij deze controles eveneens automatisch kunnen worden uitgevoerd.

Met de komst van de Chipkaart lijkt een ideaal intermediair gevonden om de gewenste controles geautomatiseerd uit te voeren.

In het navolgende artikel worden de eisen en randvoorwaarden geïnventariseerd die van toepassing zijn op het gebruik van Chipkaarten voor identifikatie van personen in gesloten en open gebruikers groepen.

Wat is een chipkaart

Een Chipkaart bestaat uit een plastic drager ter grootte van een bankkaart met een ingebedde geheugen- of microprocessor-chip.
Een chipkaart is net zo dun als een bankkaart en moet voldoen aan de ISO-normen voor Identifikatiekaarten. Daarbij wordt een betrouwbare werking geeist bij proeven voor buiging, torsie, temperatuurbereik en gevoeligheid voor vocht.

Om aan deze eisen te kunnen voldoen hanteren de fabrikanten op dit moment een maximum grootte van ongeveer 24 vierkante milimeter voor de chip in een chipkaart. Op dat kleine oppervlak moet het geheugen worden ondergebracht en, in het geval van een processor chipkaart, ook nog een microprocessor, een werkgeheugen en een programmageheugen. Vooral het werkgeheugen, ook wel Random Access Memory of kortweg RAM genoemd, neemt veel ruimte in.

De flexibiliteit van het chip-ontwerp wordt dus beperkt door de maximum grootte van het chip-oppervlak: de fabrikanten moeten een keuze doen voor een bepaalde funktionaliteit, afhankelijk van de bijbehorende kombinatie van geheugentypen.

Soorten geheugens

Bij chipkaarten komen meestal de volgende geheugentypes voor:

- RAM — Random Access Memory of Werkgeheugen is goed voor rekenfaciliteiten; waarden variëren van 36 tot 256 bytes (1 byte = 8 bits);
- (E)PROM — (Erasable) Programmable Read Only Memory wordt gebruikt als geheugen voor programma's en vastleggen van transaktieresultaten; waarden variëren van 256 bits tot 64 kbits;
- EEPROM — Electrically Erasable PROM kan tot 10.000 maal herschreven worden en aanvullend als RAM en EPROM worden gebruikt; waarden variëren van 1 tot 8 kbits.

Soorten chipkaarten

Er zijn globaal twee soorten chipkaarten te onderscheiden: Geheugen-chipkaarten en Processor-chipkaarten.

Een Geheugen-chipkaart is meestal van het type EPROM, wat in de praktijk betekent dat er alleen éénmalig in geschreven kan worden, zodat het geheugen na enige tijd "vol" is.

Een Processor-chipkaart bevat een microprocessor en heeft daarvoor werkgeheugen (type RAM) en programmageheugen (type EPROM) nodig; de kaart kan rekenen en vergelijken en heet daarom "intelligente chipkaart".

Beide soorten chipkaarten kunnen additioneel ook EEPROM geheugen bevatten. Bij de Geheugen-chipkaart

geeft dat de mogelijkheid om biometrische persoonsgegevens opnieuw te schrijven zodat langzame veranderingen gevolgd kunnen worden. Bij Processor-chipkaarten kan het programma gewijzigd worden zonder een nieuwe chipkaart uit te hoeven geven.

Organisatie van het geheugen
Het geheugen kan op allerlei manieren georganiseerd zijn, maar door de International Organisation for Standardisation (aangeduid als ISO) is voor Processor-chipkaarten een funktionele ordening in Data Files (geheugen partities) vastgesteld. Volgens ISO moeten er twee soorten Data Files worden onderscheiden:

- CDF Common Data File kan alleen beschreven worden door de kaartuitgevende instelling, maar kan door alle kaartontvangende instellingen worden gelezen om te weten welke funkties de kaart kan uitvoeren; er is maar één CDF op een kaart;

- ADF Application Data File kan alleen beschreven worden door de dienstverlenende instelling die de geheugen partitie heeft gekocht van de kaartuitgevende instelling; als er meer dan één ADF op een kaart voorkomt, zijn ze van elkaar geïsoleerd door cryptografische middelen.

controle CDF	geheugen CDF
controle ADF 1	geheugen ADF 1
controle ADF 2	geheugen ADF 2

Fig. 1 Organisatie Geheugen

Beveiliging geheugens
De beveiliging van de geheugens gebeurt met de volgende methoden:
- de chipkaart vergelijkt een aangeboden Persoonlijk Identifikatie Nummer (PIN) of wachtwoord met een in het geheugen opgeslagen waarde; als de waarden gelijk zijn mag het geheugen gelezen en eventueel beschreven worden (statische toegangscontrole);
- de chipkaart verifieert een aangeboden vercijferd gegeven door herberekening en test zodoende of de aanbieder over de geheime sleutel beschikt; bij positieve verifikatie wordt het geheugen toegankelijk (dynamische toegangscontrole).

Statische toegangscontrole heeft altijd een risico dat het aangeboden PIN of wachtwoord is gecompromitteerd en door een fraudeur opnieuw wordt aangeboden (replay).

Wat is nodig voor identifikatie?
Bij identifikatie is het een gouden regel om de kombinatie van twee kenmerken te laten gelden als criterium voor positieve identifikatie:
A. Je hebt wat;
en
B. Je bent wat.

Bij kenmerk A. hoort het bezit van een "pasje", zoals een strippenkaart, toegangsbewijs, enz.
Als voor identifikatie alleen een pasje gebruikt wordt, dan is het overdraagbaar, want het is niet persoonsgebonden. Om duplikaten uit te sluiten moet er een goed echtheidskenmerk in een pasje zitten, bijvoorbeeld een watermerk, een uniek fysiek kenmerk of een dynamisch controleerbaar cryptografisch kenmerk.

Bij kenmerk B. hoort een persoonlijk kenmerk, zoals een PIN of een biometrisch gegeven. Het PIN is eigenlijk niet zo'n goed persoonlijk kenmerk, want het is overdraagbaar, je kunt het uitlenen. Een uitgeleend of afgekeken PIN kun je nooit meer terugvragen.

Een biometrisch gegeven, zoals iemands uiterlijk of handtekening is niet overdraagbaar. Visuele controle is echter niet langer uitvoerbaar in een wereld waar "Electronic Data Interchange" (EDI) in de plaats moet komen van schriftelijke overboekingen en papieren afdekking van transakties.
Daarom wordt voor identifikatie steeds meer gewerkt met digitale registratie en automatische controle van een biometrisch gegeven. Hiervoor komen in aanmerking de stem, het netvliespatroon, dynamische handtekening-parameters, enz. Probleem hierbij is de opslag van de digitale registratie van de biometrische gegevens.

De oplossing die in dit artikel wordt toegelicht is opslag op een chipkaart bij wijze van het onder A. genoemde pasje. Door die digitale registratie cryptografisch te beveiligen is aan alle identifikatie-eisen voldaan: het pasje is niet overdraagbaar, het is "echt" en je kunt het alleen gebruiken als de legale kaarthouder zijn/haar biometrische eigenschappen laat meten.

Afhankelijkheid van de omgeving
Er moet onderscheid gemaakt worden in eisen aan identifikatie binnen en buiten de eigen organisatie.

Binnen de eigen organisatie is er meestal sprake van een homogene en stuurbare infrastruktuur. Er is bijvoordeeld een gesloten gebruikersgroep met een eigen netwerk, de PC's werken allemaal met hetzelfde besturingssysteem en zijn van hetzelfde merk, enz.
De gekozen identifikatiemethode kan dan komponenten omvatten die met dat merk PC werken, wat onmogelijk zou zijn als allerlei PC-merken waren toegestaan.

Buiten de eigen organisatie is er een open gebruikersgroep, de infrastruktuur is heterogeen, de PC's en besturingssystemen zijn niet te sturen en er worden allerlei communicatiewegen gebruikt.

In dit laatste geval zal er meer dan één identifikatiemethode moeten worden aangeboden of de gekozen methode zal beperkt moeten blijven tot produkten met een genormaliseerde aansluiting, zoals chipkaartlezers die met een RS-232 aansluiting aan iedere PC gekoppeld kunnen worden.

Kortom, binnen de eigen organisatie kan de keuze voor een identifikatiemethode geavanceerder en duurder zijn dan bij een open gebruikersgroep, omdat in het eerste geval het beheer van de identifikatiemiddelen (zoals chipkaarten en lezers) uitvoerbaar blijft.

Bedreigingen en funkties

Aanvallen waarmee rekening gehouden moet worden bij het kiezen van een identifikatiemethode zijn:

- Interceptie van de identiteit met als gevolg dat de dader zich uitgeeft voor de identiteithouder door middel van maskerade en replay;
- Interceptie van een bericht met als gevolg dat het bericht door onbevoegden gelezen kan worden;
- Manipulatie van een bericht, waardoor de ontvanger een vervalst bericht krijgt;
- Ontkenning van het zenden van een bericht, waardoor de ontvanger de geleden schade niet kan verhalen.

In onderstaande matrix staan de beveiligingsfunkties die tegen de genoemde aanvallen worden aangewend.

BEDREIGINGEN	BRON AUTHENTIKATIE	BERICHTAUTHENTIKATIE	CONFIDENTIALITEIT	NON REPUDIATION
INTERCEPTIE (Identiteit)	X			
INTERCEPTIE (Bericht)			X	
MASKERADE	X			
REPLAY	X			
MANIPULATIE		X		X
LOOCHENEN				X

Fig. 2 Bedreigingen en beveiligingsfunkties

De werking van de beveiligingsfunkties is als volgt:

- Bron authentikatie bewijst de echtheid van de bron en synchroniseert het begin van een sessie;
- Bericht authentikatie bewijst de integriteit en de herkomst van een afzonderlijk bericht;
- Confidentialiteit vercijfert een bericht;
- Non repudiation geeft de ontvanger het bewijs dat de zender een bericht verzonden heeft; een derde partij kan dit bewijs controleren zonder de geheime sleutel van de zender te kennen.

Er is verschil tussen bron authentikatie en bericht authentikatie. Bron authentikatie waarborgt alleen de echtheid van de bron onmiddellijk na het uitvoeren ervan. Bij bericht authentikatie is voor ieder afzonderlijk bericht de bron en de integriteit gewaarborgd, maar een replay aanval is nog steeds mogelijk. Daarom kan aan het bericht een datum/tijd of een volgorde nummer worden toegevoegd, zodat dubbele en missende boodschappen worden gedetekteerd. Maar hoe kom je weer tot nummer synchronisatie na een onherstelbare volgorde fout? Het antwoord hierop is het kombineren van bron authentikatie (herstel synchronisatie) en bericht authentikatie (handhaven berichtvolgorde).

Identifikatie en authentikatie met de chipkaart

Identifikatie van een persoon door middel van een chipkaart heeft niet alleen zin voor toegangscontrole, maar ook om, met name in het geval van EDI, de integriteit en de herkomst van een bericht te waarmerken, te voorzien van een elektronische handtekening.

De rol van de chipkaart bij de beveiliging van de bron en van de data wordt gemeten aan de hand van de beveiligingsprestatie, m.a.w. welk type chipkaart kan welke bedreigingen oplossen.

Beveiligingsprestatie van de Geheugen-chipkaart

Er moet onderscheid gemaakt worden tussen twee typen Geheugen-chipkaarten:

- Geheugen-chipkaart met eenmalige opslag van data (EPROM):
  * eenvoudige bron-authentikatie door PIN-controle en het terugschrijven van steeds een nieuwe variabele om een replay te voorkomen; de online host controleert bij iedere verifikatie de laatst bijgeschreven variabele;
  * eindige bescherming tegen replay door "vol" raken van het geheugen in de chipkaart waar de variabele wordt opgeslagen;
- Geheugen-chipkaart met herschrijfbare opslag van data (EEPROM):
  * eenvoudige bron-authentikatie door PIN-controle en opslag van variabele tegen replay (als hierboven);
  * blijvende bescherming tegen replay door herschrijfbaar geheugen.

Beveiligingsprestatie van de Processor-chipkaart

Er moet onderscheid gemaakt worden tussen twee typen Processor-chipkaarten:

- Processor-chipkaart met symmetrisch algoritme:
  * cryptografische bron-authentikatie door een challenge-response proces (zie hierna);
  * bericht-authentikatie door Message Authentication Code (MAC volgens ISO norm IS 8730 of ANSI X9.9);
  * data confidentialiteit (met Data Encryption Algorithm van ANSI X3.92 en procedures voor bericht-vercijfering volgens ISO 10126-1 en -2).

- Processor-chipkaart met asymmetrisch en symmetrisch algoritme:
  * cryptografische bron-authentikatie zonder geheime sleutel door asymmetrische challenge-response;
  * bericht-authentikatie door Hashing (ISO 10118-2) en Signing (ISO 9796) van het Hash-resultaat; bij een hash-funktie is het rekenkundig niet doenlijk om nog een zinvol bericht te vinden dat tot hetzelfde Hash-resultaat leidt;
  * data confidentialiteit (met Data Encryption Algorithm net als bij symmetrisch);
  * non repudiation met Signing en eventueel Hashing net als bij bericht-authentikatie.

Processchema's voor bron- en bericht-authentikatie

Hierna wordt voor de Processor-chipkaart in fig. 3 een schema voor bron-authentikatie (symmetrisch) gegeven en in fig. 4 een schema voor non repudiation.



Fig. 3: Processor-chipkaart (symmetrisch), bron-authentikatie

In figuur 3 genereert de controleur eerst R, een voor de vrager onvoorspelbare "challenge". De controleur verzendt de challenge en de vrager berekent oK(R) met geheime sleutel K en met input R. Hierbij is oK(R) een funktie waarbij uit het resultaat niet af te leiden is welke sleutel er is gebruikt (one-way algoritme). De vrager verzendt oK(R) en de controleur berekent inmiddels zelf de waarde oK(R)'. Als beide waarden gelijk zijn is de vrager authentiek. Voorwaarde voor deze funktie is dat vrager en controleur beiden beschikken over dezelfde geheime sleutel K.



Fig. 4: Processor-chipkaart (asymm./symm.), non repudiation

In figuur 4 berekent de zender eerst H, het resultaat van de hash-funktie van het bericht. De zender "tekent" het bericht door de signing-funktie met de geheime sleutel S van een asymmetrisch algoritme op H toe te passen (bijvoorbeeld het Rivest/Shamir/Adleman ofwel het RSA algoritme). De zender verzendt het getekende bericht sS(H) (= Sig) en de controleur verifieert met de openbare sleutel P en met input Sig.

Hierbij is

vP(Sig) = vP(sS(H)) = H'

als RSA gebruikt wordt.
Als H' gelijk is aan H, dan is het bericht authentiek en afkomstig van de zender. De zender kan ook niet ontkennen dat het bericht van hem/haar afkomstig is, want alleen de zender beschikt over de geheime sleutel. Bovendien kan iedere derde partij de verifikatie uitvoeren.

Praktische toepassingen

Bij de praktische toepassing van chipkaarten voor identifikatie en authentikatie zijn de volgende faktoren doorslaggevend voor de gekozen oplossing:
- er moet aan het vereiste minimum beveiligingsniveau voldaan kunnen worden;
- er moet een reële verhouding bestaan tussen de kosten voor de beveiliging en het afgedekte risico;
- de beveiligingsprestatie van de chipkaart moet toereikend zijn;
- de gekozen oplossing moet gebruiksvriendelijkheid zijn en een goede promotie hebben.

Hieronder worden een paar toepassingen behandeld voor verschillende typen chipkaarten.

Geheugenchipkaart als telefoonkaart

In Frankrijk en Duitsland worden maandelijks al enige tientallen miljoenen Geheugen-chipkaarten gebruikt om te telefoneren. Deze wegwerpkaart werkt zonder PIN en de kaart wordt van tevoren betaald. Verlies van de kaart betekent het verlies van de telefoontikken.
Het telefoontoestel controleert met een asymmetrisch algoritme de (statische) echtheidscode van de kaart.

Geheugen-chipkaart voor PC-Hostbeveiliging

* Beveiliging kaarthouder door kombinatie van Wachtwoord en vercijferde sleutels in de chipkaart;
* Beveiliging systeemsoftware door encrypte diskdrive; de vercijferde software op floppy disks wordt ontcijferd door een encryptor bord op de PC m.b.v. vercijferde sleutels in de Geheugen-chipkaart.

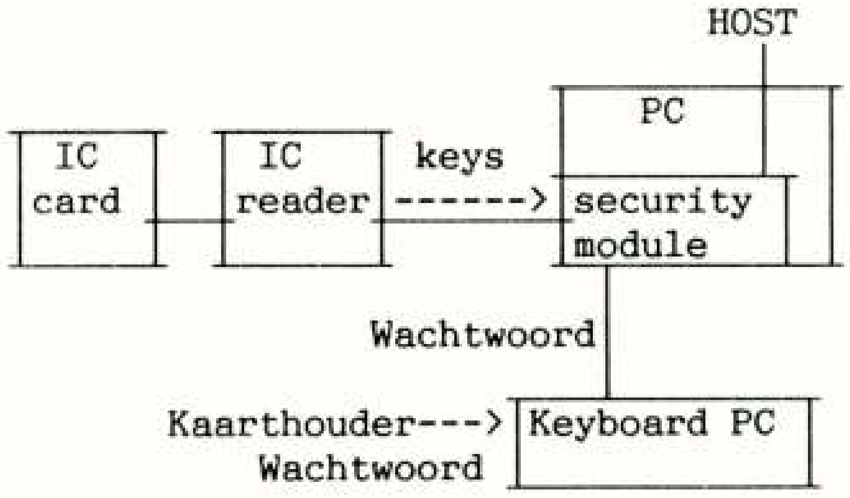


Fig. 5: Geheugen-chipkaart, PC-Hostbeveiliging

Processor-chipkaart voor elektronisch bankieren

Voor elektronisch bankieren gebruiken verschillende banken in Nederland een Processor-chipkaart die m.b.v. een symmetrisch algoritme authentikatie van de bron en van de te accorderen berichten uitvoeren:

* Beveiliging kaarthouder door PIN in chipkaart en mogelijkheid bron-authentikatie van het systeem;
* Beveiliging systeem door bron authentikatie door challenge/response met geheime sleutel in chipkaart;
* data authentikatie;
* data confidentialiteit.

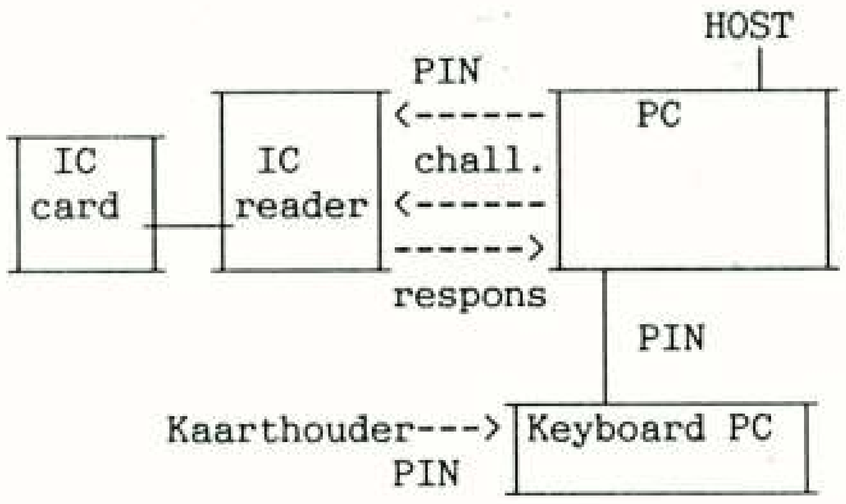


Fig. 6: Processor-chipkaart elektronisch bankieren

Processor-chipkaart voor EDI

Voor Electronic Data Interchange (EDI) met asymmetrisch algoritme zou een nog te ontwikkelen chipkaart de volgende opzet geven:

* Beveiliging kaarthouder door PIN in Chipkaart en mogelijkheid bron-authentikatie van het systeem;
* Beveiliging systeem door bron authentikatie met digital signature zonder geheime sleutel in systeem;
* data authentikatie;
* data confidentialiteit;
* non repudiation.

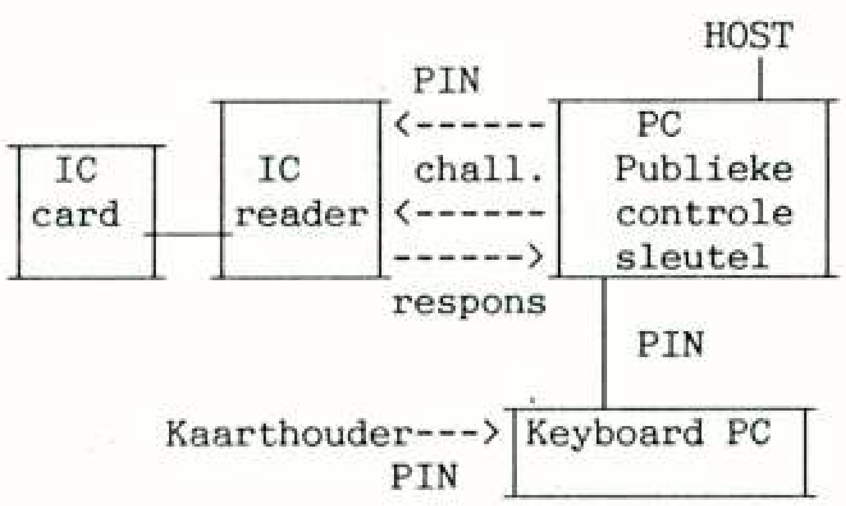


Fig. 7: Processor-chipkaart voor EDI

ISO referenties

ISO 10202/1 FINANCIAL TRANSACTION CARDS - Security Architectures of Financial Transaction Systems using Integrated Circuit Cards - CARD LIFE CYCLE.

ISO 10202/2 FINANCIAL TRANSACTION CARDS - Security Architectures of Financial Transaction Systems using Integrated Circuit Cards - TRANSACTION PROCESS

ISO 10202/3 FINANCIAL TRANSACTION CARDS - Security Architectures of Financial Transaction Systems using Integrated Circuit Cards - CRYPTOGRAPHIC KEY RELATIONSHIPS

ISO 10202/4 FINANCIAL TRANSACTION CARDS - Security Architectures of Financial Transaction Systems using Integrated Circuit Cards - SECURITY MODULES

ISO 10202/5 FINANCIAL TRANSACTION CARDS - Security Architectures of Financial Transaction Systems using Integrated Circuit Cards - USE OF ALGORITHMS

ISO 10202/6 FINANCIAL TRANSACTION CARDS - Security Architectures of Financial Transaction Systems using Integrated Circuit Cards - CARDHOLDER VERIFICATION

ISO 9796 Information Technology - Security Techniques - Digital signature scheme giving message recovery

ISO 10118/1 Data Cryptographic Techniques - Hash-functions for digital signatures and authentication mechanisms; part 1 - General

ISO 10118/2 Data Cryptographic Techniques - Hash-functions for digital signatures and authentication mechanisms; part 2 - Hashing operation using a symmetric block cipher algorithm

DIS 9594-8 Information processing systems - Open Systems Interconnection - The Directory - Part 8: Authentication Framework

ISO 9797 Data Cryptographic Techniques - Data integrity mechanism using a cryptographic check function employing a block cipher algorithm

ISO 9798/1 Data Cryptographic Techniques - Entity authentication mechanisms, Part 1: General model for entity authentication mechanisms

ISO 9798/2 Data Cryptographic Techniques - Entity authentication mechanisms, Part 2: Entity authentication using symmetric key techniques

ISO 9798/3 Data Cryptographic Techniques - Entity authentication mechanisms, Part 3: Entity authentication using public key techniques

ISO 10116 Data Cryptographic Techniques - Modes of operation for an n-bit block cipher algorithm

ISO 9992 Financial transaction cards - messages between the ICC and the CAD:

Part 1 Concepts and structures
Part 2 Functions
Part 3 Messages (commands and responses)
Part 4 Common data for interchange
Part 5 Data elemants

ISO 9807 Message Authentication (Retail)

Voordracht gehouden tijdens de 382e werkvergadering.



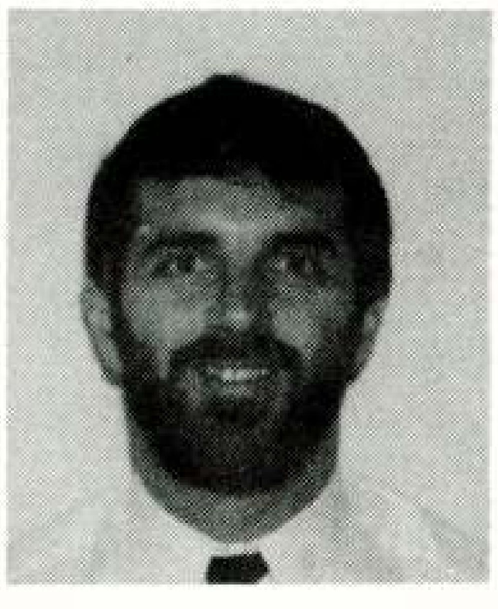
IR. O. B. M. PIETERSEN

NEDERLANDS ELECTRONICA- EN RADIOGENOOTSCHAP
THE INSTITUTION OF ELECTRICAL AND ELECTRONICS ENGINEERS
BENELUX SECTION
(383e WERKVERGADERING)

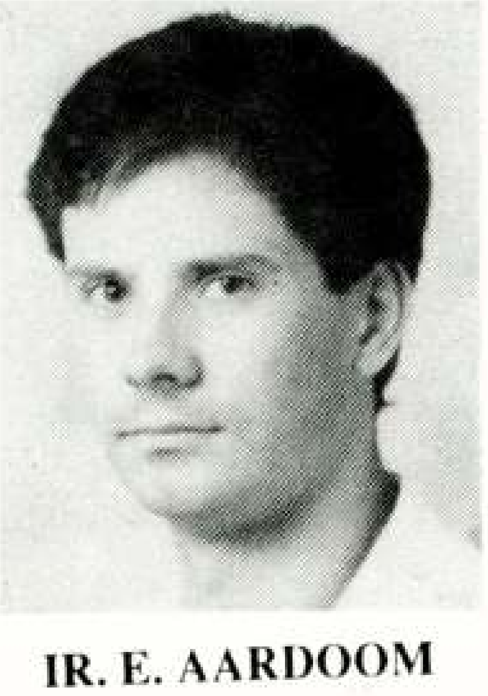
UITNODIGING

voor de lezingendag op **dinsdag 6 november 1990** op het **Nationaal Lucht- en Ruimtevaart Laboratorium** in de **Noordoostpolder** (nabij Vollenhove).

ONDERWERP: SATELLIETNAVIGATIE - NAVSTAR GPS -



CHR. MOYLE



IR. E. AARDOOM

PROGRAMMA:

9.45 uur:	Ontvangst
10.15 uur:	NAVSTAR GPS - INSTRUCTION AND STATUS -; **IR. O. B. M. PIETERSEN,** Nationaal Lucht- en Ruimtevaart Laboratorium NLR
10.30 uur:	GPS RECEIVERS FOR MILITARY PLATFORMS; **CHR. MOYLE,** GEC-Plessey Avionics Ltd, United Kingdom
11.15 uur:	Pauze
11.45 uur:	CAPABILITIES OF GPS FOR AVIATION APPLICATIONS; **DRS N. VAN DRIEL,** Nationaal Lucht- en Ruimtevaart Laboratorium NLR
12.30 uur:	UITREIKING VEDERPRIJS AAN **DR. IR. R. J. VAN DE PLASSCHE.** De considerans zal worden uitgesproken door Prof. Ir. A. Kok
13.00 uur:	Lunch, aangeboden door het NLR
14.00 uur:	DESIGN AND REALISATION OF A CIVIL NAVSTAR RECEIVER; **IR. E. AARDOOM,** TU Delft, Faculteit Elektrotechniek, vakgroep Electronische Techniek
14.45 uur:	Theepauze
15.00 uur:	GPS, A NEW TOOL IN THE FIELD OF LANDSURVEY AND LANDNAVIGATION - A SURVEY OF APPLICATION POSSIBILITIES AND RESULTS OBTAINED SO FAR -; **IR. J. H. M. VAN DER WAL EN IR. G. M. LAMMERTS VAN BUEREN,** Meetkundige Dienst van Rijkswaterstaat
15.45 uur:	Sluiting.

Aanmelding voor deze dag dient te geschieden vóór 15 oktober door middel van aangehechte kaart, gefrankeerd met een postzegel van 55 cent. Het aantal deelnemers is beperkt; tijdstip van ontvangst van aanmelding is beslissend voor deelname. Als blijkt dat u, na uw aanmelding, niet kunt deelnemen aan deze lezingendag, ontvangt u hierover van ons bericht.

Namens de samenwerkende verenigingen,
ir. N. H. G. Baken, NERG
tel. 070 - 332 64 82

Leidschendam, september 1990.

NAVSTAR GLOBAL POSITIONING SYSTEM

- Introduction and Status -

O.B.M. Pietersen

Nationaal Lucht- en Ruimtevaartlaboratorium NLR

A general description is given of the Navstar Global Positioning system. After a systems overview the technical characteristics of the Space- Control- and User Segment are described. The status of the three segments is given as existing at the end of 1990.

The text of this article has been based for the greater part on the first chapter of the Nato publication ANP-2: "Introduction to Navstar GPS User Equipment", written by the Nato Team in Los Angeles. It has been amended however by the author with system status data as per December 1990 and accuracy data from Draft NATO STANAG 4294, "Navstar GPS System Characteristics".

GPS SYSTEM OVERVIEW

1. General System Description

The NAVSTAR Global Positioning System (GPS) is a space based radio positioning system which provides suitably equipped users with highly accurate position, velocity and time data. When fully operational, this service will be provided globally, continuously, and under all weather conditions to users at or near the surface of the earth. GPS receivers operate passively, thus allowing an unlimited number of simultaneous users. The GPS has features which can deny accurate service to unauthorized users, prevent spoofing and reduce receiver susceptibility to jamming. System Performance is described in more detail in paragraph 4.

The GPS comprises three major segments Space, Control and User. The Space Segment consists of a constellation of GPS satellites in semisynchronous orbits around the earth. Each satellite broadcasts radio-frequency (RF) ranging codes and a navigation data message. The Control Segment consists of a Master Control Station (MCS) and a number of monitor stations located around the world. The MCS is responsible for tracking, monitoring, and managing the satellite constellation and updating the navigation data messages. The User Segment consists of variety of radio navigation receivers specifically designed to receive, decode and process the GPS satellite ranging codes and navigation data messages. The Space, Control and User Segments are described in more detail in paragraph 2.

The ranging codes broadcast by the satellites enable a GPS receiver to measure the transit time of the signals and thereby determine the range between a satellite and the user (see figure 1). The navigation data message enables a receiver to calculate the position of each satellite at the time of transmission of the signal. Four satellites are normally required to be simultaneously "in view" of the receiver for three-dimensional (3-D) positioning purposes. This allows the user 3-D position coordinates and the user clock offset to be calculated from the satellite range and position data. Treating the user clock offset as an unknown eliminates the requirement for users to be equipped with precision clocks. Less than four satellites can be used if the user altitude or system time is precisely known. A more detailed explanation of the GPS theory of operation is provided in paragraph 5.

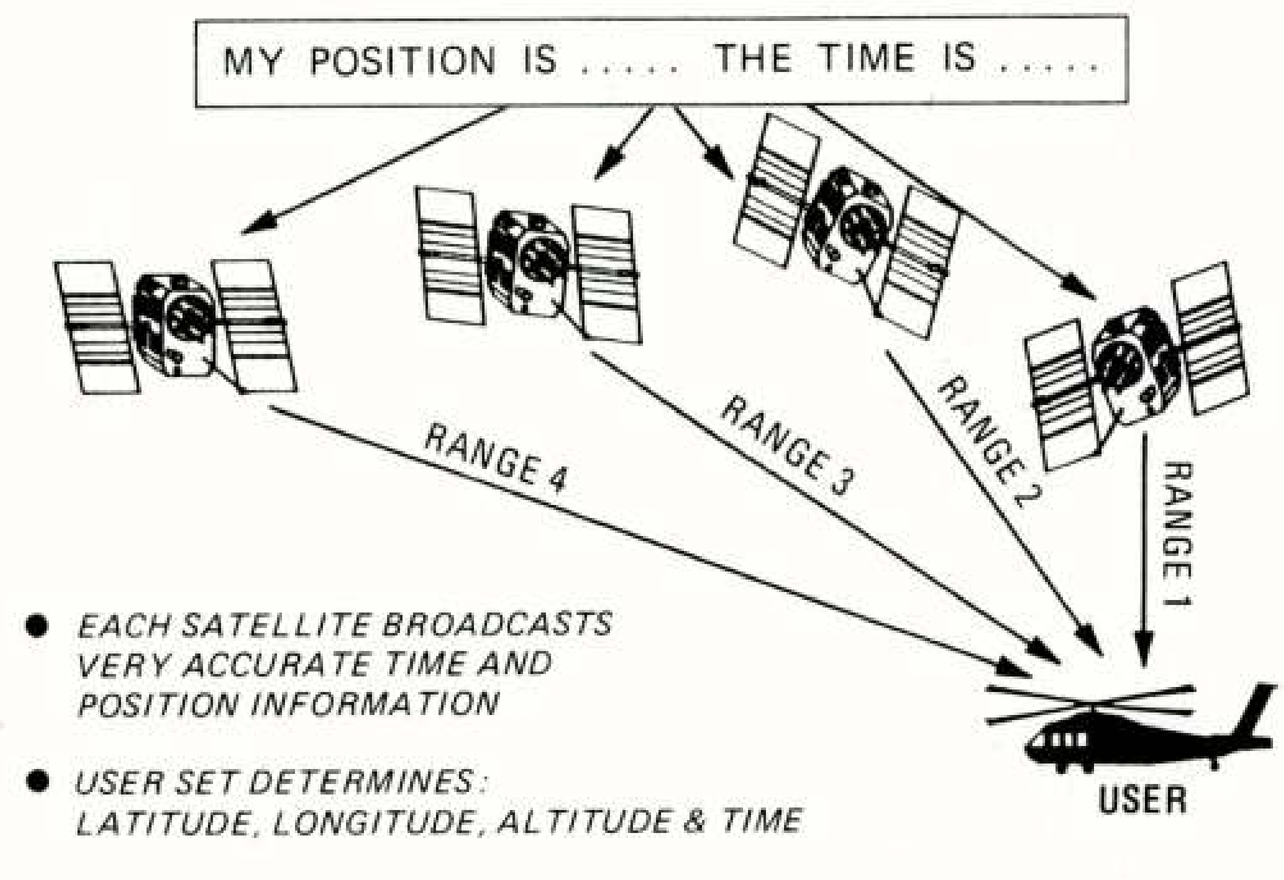


Fig. 1 How GPS works

2. System Technical Description

2.1 Space Segment

The GPS Space Segment, when fully operational, will consist of 21 operational satellites (see figure 2). To ensure system availability, three additional satellites will be orbited as active spares. The satellites will be placed in six orbital planes with four satellites in each plane. The satellite orbital planes will have an inclination relative to the equator of 55 degrees and the height will be 20200 km (see figure 3). The satellites will complete an orbit in approximately 12 hours.

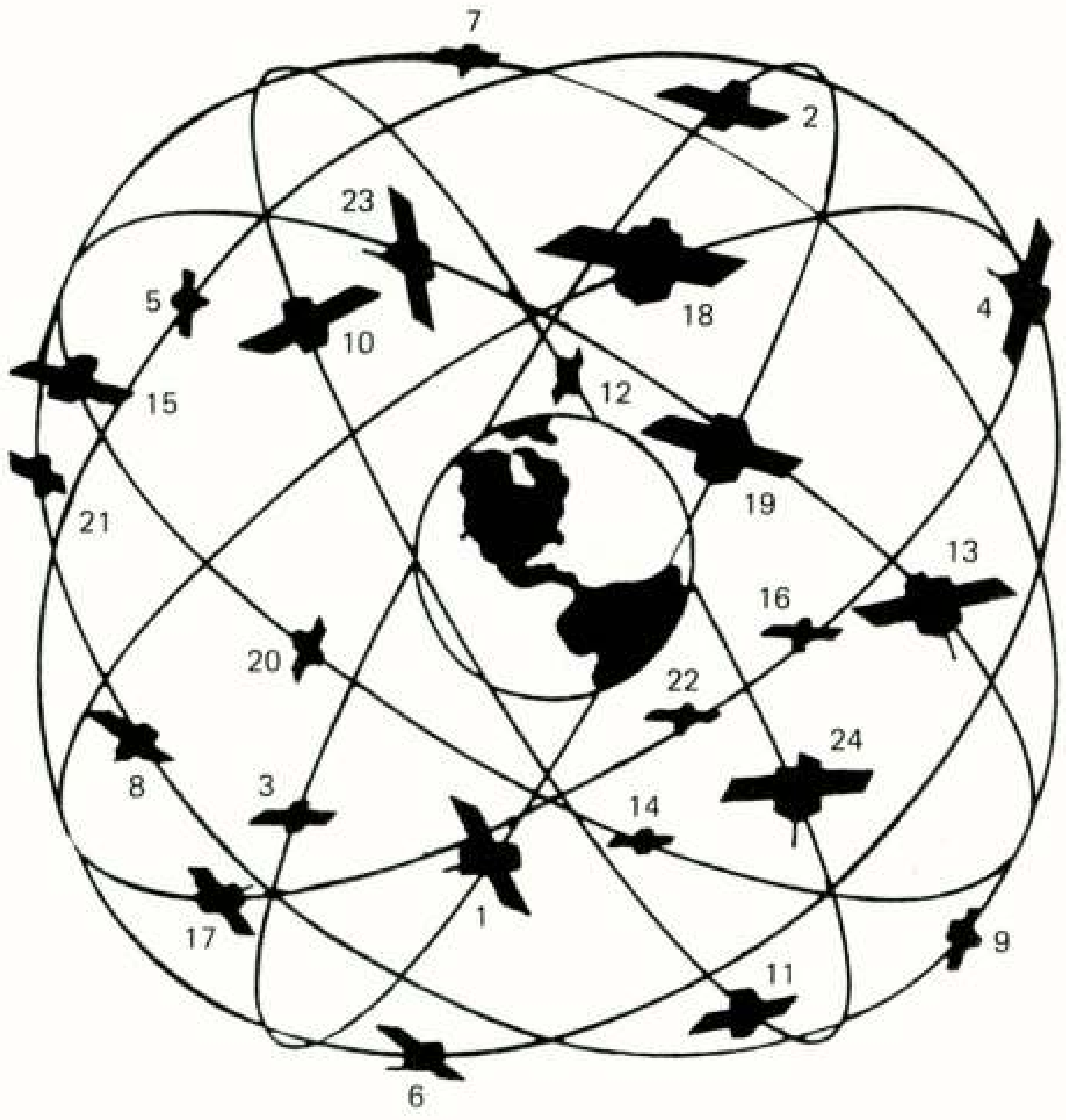


Fig. 2 The Navstar operational satellite constellation

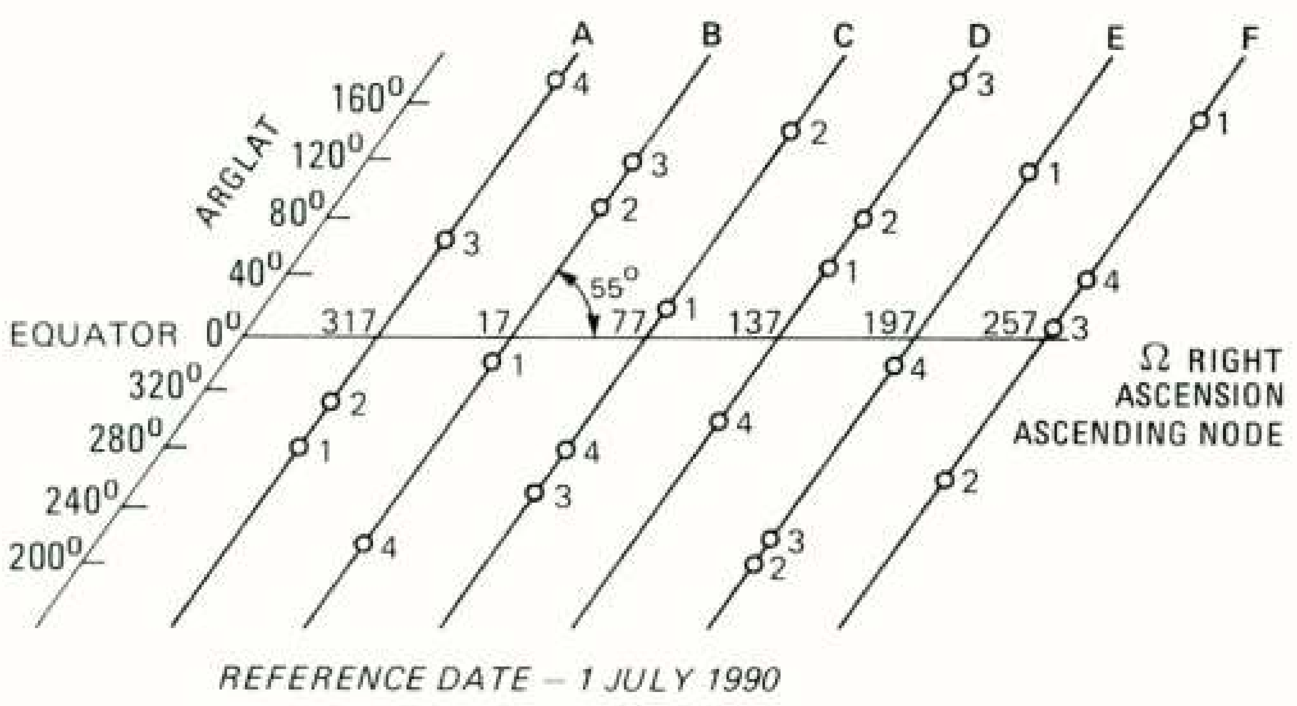


Fig. 3 Position in orbit of the 21 operational and 3 active spare satellites

An observer on the ground will observe the same satellite ground track each day; however the satellites will become visible 4 minutes earlier each day due to a 4 minute/day difference between the satellite orbit time and the rotation of the earth. The satellites will be positioned such that a minimum of 5 satellites will normally be observable by a user anywhere on earth. The satellites transmit on two frequencies: L1 = 1575.42 MHz and L2 = 1227.6 MHz. The satellites transmit their signals using spread spectrum techniques, employing two different spreading functions a 1.023 MHz course/acquisition (C/A) code on L1 only and a 10.23 MHz precision (P) code on both L1 and L2. The minimum signal power for the different signals at a GPS receiver (RCVR) antenna will be as follows:

L_1, C/A code: -160 dBW
L_1, P code : -163 dBW
L_2, P code : -166 dBW

Both P-code and C/A-code enable a RCVR to determine the range between the satellite and the user. Superimposed on both the P-code and the C/A-code is the NAVIGATION-message (NAV-msg), containing satellite ephemeris data, atmospheric propagation correction data, and satellite clock-bias information. See paragraph 5 for additional details regarding the ranging codes and NAV-msg.

2.2 Control Segment

The control segment consists of one Master Control Station (MCS) at Falcon AFS in Colorado Springs, USA, plus monitor stations at the MCS, Hawaii, Kwajalein, Diego Garcia and Ascension (see figure 4). All monitor stations, except Hawaii and Falcon, are equipped with ground antennas for communications with the GPS satellites (see figure 5). The monitor stations passively track all GPS satellites in view, collecting ranging data from each satellite. This information is passed on to the MCS where the satellite ephemeris and clock parameters are estimated and predicted. The MCS periodically uploads the ephemeris and clock data to each satellite for retransmission in the NAV-msg.

2.3 User Segment

The User Segment consists of a variety of military and civilian GPS receivers specifically designed to receive, decode and process the GPS satellite signals. They include stand-alone receiver sets, as well as equipment that is integrated with or embedded into other systems. They serve a variety of user applications including navigation, positioning, time transfer, surveying and attitude reference. Consequently, GPS receivers for different applications can vary significantly in design and function.

3. Program history and present status

After a concept validation phase, Phase I, (1973-1979) a full scale development and system test phase, Phase II, began in 1980. Between 1978 and 1985 10 successfull launches of Block I satellites occurred, of which 6 are still usable (December 1990). In September 1980 IBM was awarded a contract to build an Initial Control System (ICS), an interim system to fill the gap between the Phase I Control System and the final Operational Control System (OCS). The ICS was located at Vandenberg AFB. At the same time IBM was also awarded the contract to design and develop the OCS.

Phase II for the User Segment was divided into two phases Phase IIA and Phase IIB. In Phase IIA, starting in July 1979, four contractors Magnavox, Rockwell-Collins, Texas Instruments and Teledyne were awarded contracts to carry out performance analyses and preliminary design of UE. In 1982 Rockwell-Collins and

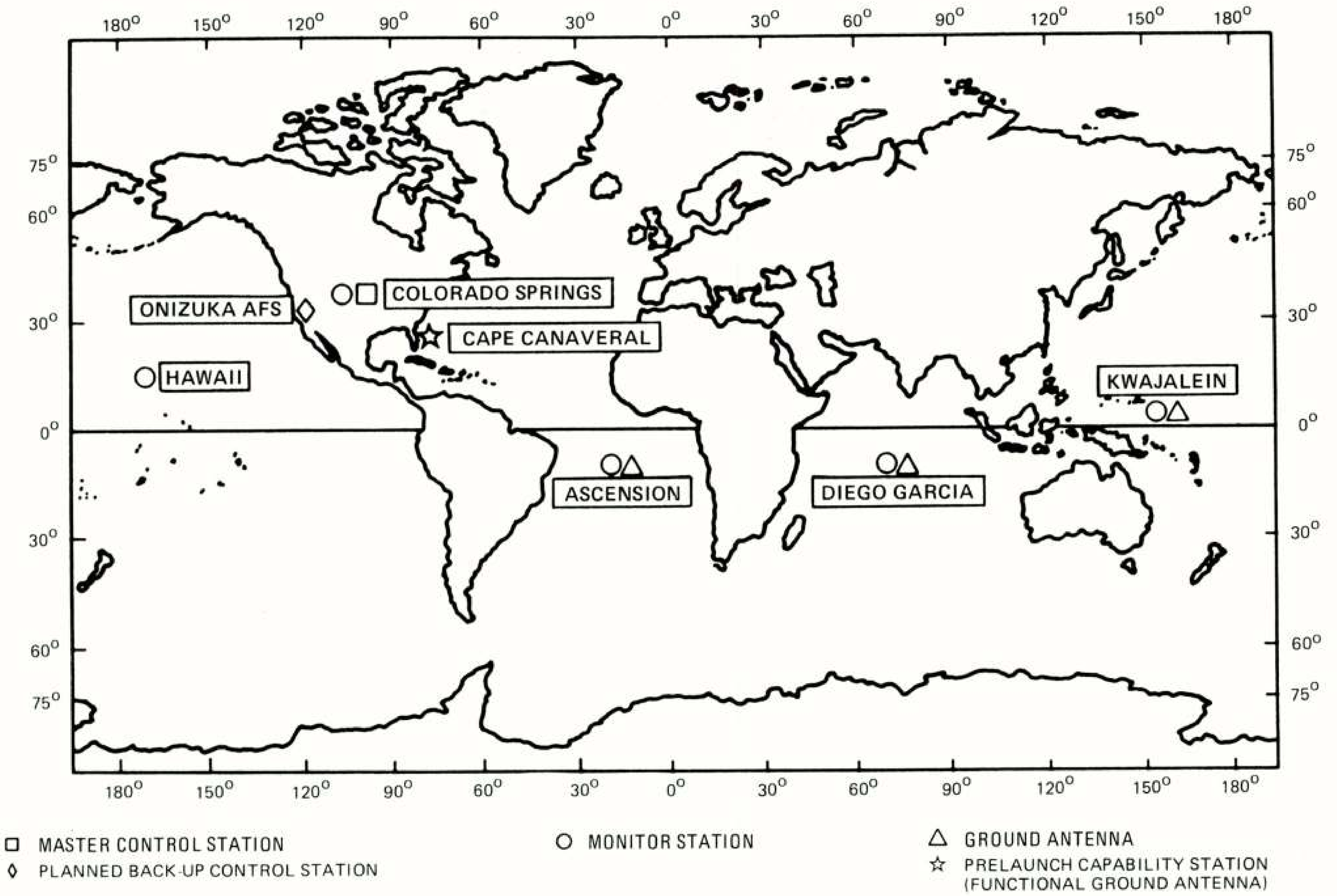


Fig. 4 The operational control system

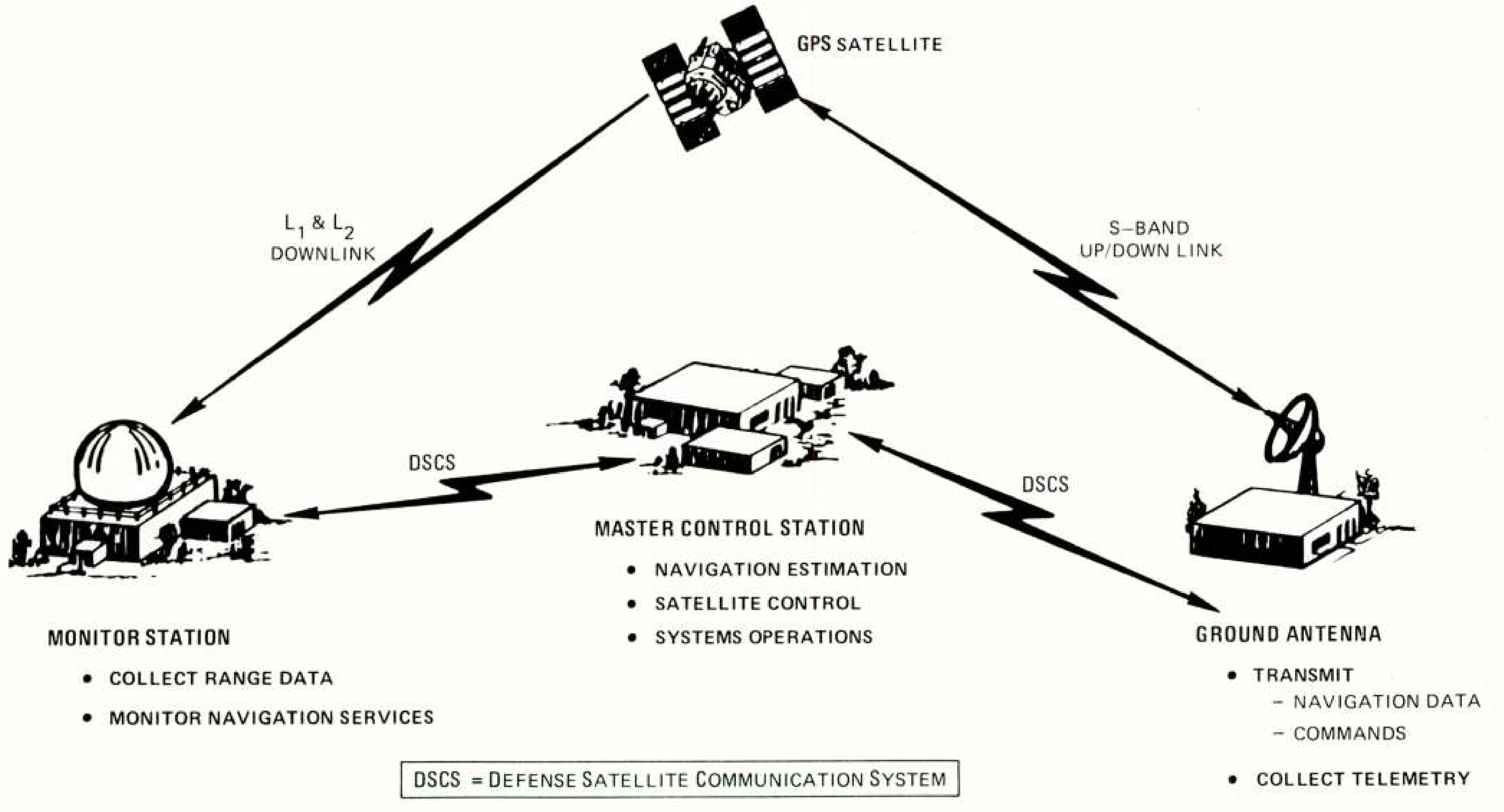


Fig. 5 Links between satellites, monitor stations, ground antennas and master control station

Magnavox were selected to continue into Phase IIB which required continued design refinement, fabrication of prototype GPS UE, qualification testing and extensive field testing of the UE.

A contract for 28 operational (Block II) GPS satellites was awarded to Rockwell International Corporation in 1983. Phase III, the production and deployment phase started in 1985. The first Block II satellite was launched in February 1989 aboard the Delta II medium launch vehicle (MLV). Worldwide two-dimensional positioning capability is projected for mid-1991 assuming that the remaining Block I satellites are still operational. Similarly, worldwide 3-D capability is projected for early-1993. Table 1 and figure 6 show additional details regarding Block II satellites.

BLOCK I (1978-1985) (ALL LAUNCHED)	- DEVELOPMENT SATELLITES - 11 LAUNCHED -- 1 BOOST FAILURE -- 6 CURRENTLY MISSION CAPABLE
BLOCK II (1989-1995) (10 LAUNCHED)	- 1 QUAL VEHICLE (GPS-12) - 28 OPERATIONAL SATELLITES -- SUPPORT 21 + 3 SATELLITE CONSTELLATION 10 CURRENTLY MISSION CAPABLE (DEC '90)
BLOCK IIR 1995 →	- 20 OPERATIONAL REPLENISHMENT SATELLITES (OPTIONS FOR 6 ADDITIONAL)

Tab. 1 Navstar GPS Block I, II and IIR satellites

In June of 1989 a contract was awarded to General Electric for 20 GPS replenishment satellites, designated Block IIR. The contract includes options for six additional satellites as well. Delivery of the first satellite is scheduled for October of 1994. The Block IIR satellites will have the capability for 180 day autonomous operation. In addition, a technique of ranging and communication between the Block IIR satellites (cross-link ranging) will be used to estimate and update the parameters in the navigation message of each Block IIR satellite without contact from the Control Segment.

In May 1985, IBM installed the OCS computers, software, and mission consoles at the MCS at Vandenberg AFB, California. The OCS began uploading navigation information to the satellites in October of 1985. The OCS was moved to the Consolidated Space Operations Center (CSOC) at Falcon AFB, Colorado in February 1986. Air Force Operational Test and Evaluation Command tests to verify OCS Operational capability were completed in December 1989. Formal turnover of the OCS from Systems Command to Space Command was accomplished in mid 1990.

Rockwell-Collins was selected as the contractor for the production GPS user equipment (UE) in April 1985. Low rate initial production of the GPS UE was begun and the first set was delivered to the JPO in June of 1988. By mid 1990, approximately 4500 receivers had been delivered to the U.S. In October 1990 a full-rate production contract was awarded to SCI Technology which firm will build-to-print the equipment developed by Rockwell-Collins.

In addition other procurement efforts have begun. In September 1987, a contract was awarded to Texas Instruments Incorporated to produce 5-Channel PPS C/A-code sets for use in ground vehicles and by ground personnel. The first of these receivers was delivered to the JPO for testing in November 1988. The JPO begun procurement of a miniature airborne GPS receiver (MAGR) for use in aircraft where space is severely limited. In November of 1990 a contract was awarded to Rockwell-Collins for a limited production program. The first receivers are expected to be delivered in 1994.

Phase III integration and test efforts are currently under way in the USA on a variety of host vehicles. In addition to U.S. test efforts, Australia, Canada, Denmark, the Federal Republic of Germany, the Netherlands, Norway, and the United Kingdom have also conducted test programs in cooperation with the JPO. In the Netherlands tests were (and are) carried out by the National Aerospace Laboratory NLR in the areas of anti-jamming, INS aiding and so-called differential GPS.

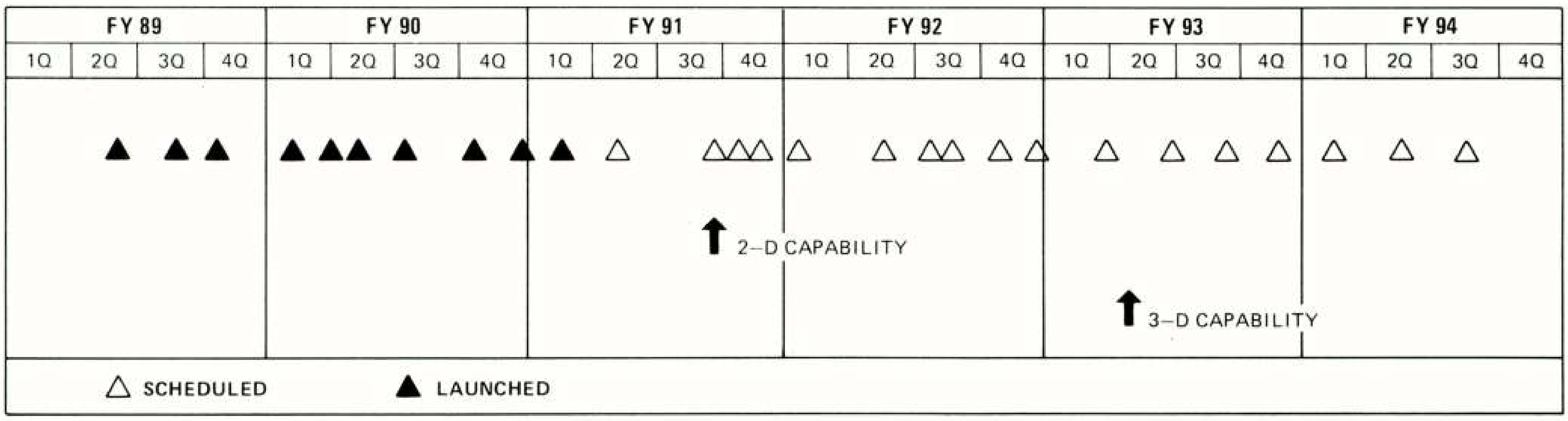


Fig. 6 GPS Block II launch schedule

Phase III of the GPS program has seen a tremendous expansion in the development and production of international and commercial user equipment. Military user equipment is being produced by participating NATO nations including Canada, France, Germany, Italy and the United Kingdom.

4. System Performance

4.1 Levels of Service

Two levels of navigation are provided by the GPS, the Precise Positioning Service (PPS) and the Standard Positioning Service (SPS). The PPS is a highly accurate positioning, velocity and timing service which is made available only to authorized users. The SPS is a less accurate positioning and timing service which is available to all GPS users (see figure 7). The accuracy of the services is determined by the User Equivalent Range Error (UERE), see table 2, multiplied by the PDOP, the Position Dilution of Precision, which is a factor dependent only on the prevailing satellite geometry. Next paragraphs give some attainable accuracy figures for both services.

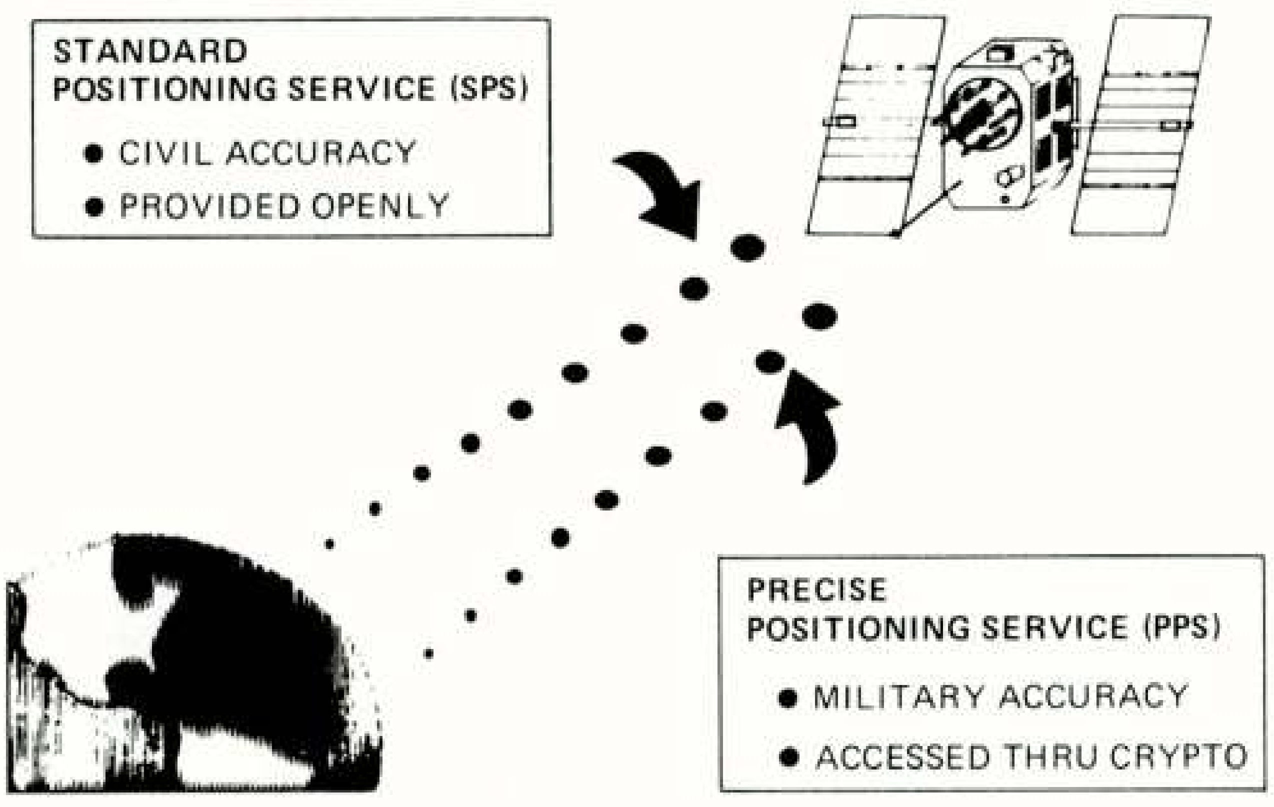


Fig. 7 GPS standard and precise positioning services (SPS and PPS)

Segment	Error Source	UERE Contribution (95 %) (m)	
		P-code	C/A-code
Space	Navigation Signal a. Frequency standard stability b. D-band delay variation	6.5 1.0	6.5 1.0
	Space vehicle acceleration uncertainty	2.0	2.0
	Other	1.0	1.0
Control	Ephemeris prediction and model implementation	8.2	8.2
	Other	1.8	1.8
User	Ionospheric delay compensation	4.5	9.8 - 19.6
	Tropospheric delay compensation	3.9	3.9
	Receiver noise and resolution	2.9	2.9
	Multipath	2.4	2.4
	Other	1.0	1.0
	95 % System UERE*	13.0	15.7 - 23.1

* Root-sum-square of all error sources

Tab. 2 User Equivalent Range Error, without SA-effects (to be multiplied with PDOP for navigation error)

4.2 Precise Positioning Service

The PPS is specified to provide 33 meter, 95 %, 3-D positioning accuracy and 100 ns (one sigma), or 180 ns, 95 %, UTC time transfer accuracy to authorized users. Sometimes the SEP, Spherical Error Probable, is quoted which is a 50 % value. This SEP is specified as 16 m. The 95 % horizontal accuracy is specified as 18 m. PPS receivers can achieve 0.2 metres per second 3-D velocity accuracy, but this is somewhat dependent on receiver design. The PPS is primarily intended for military purposes. Authorization to use the PPS is determined by the U.S. Department of Defense (DOD), based on U.S. defense requirements and international commitments. Authorized users of the PPS include U.S. Military users, NATO military users and other selected military and civilian users such as the Australian Defense Forces and the U.S. DMA.

Access to the PPS is controlled by two features using cryptographic techniques. A Selective Availability (SA) feature is used to reduce the GPS position, velocity and time accuracy available to unauthorized users. SA operates by introducing controlled errors into the satellite signals. The U.S. DOD has stated that in peace time the effects of SA will be controlled to provide 100 meter (95 %) horizontal accuracy for SPS users. System accuracy degradations can be increased if it is necessary to do so, for example, to deny accuracy to a potential enemy in time of crisis or war. An Anti-Spoofing (A-S) feature will be envoked when the system becomes operational. This feature will negate potential spoofing (hostile imitation) of PPS signals. The technique alters the P-code cryptographically into a code denoted as the Y-code (the C/A code remains unaffected). Encryption keys and techniques are provided to PPS users which allow them to remove the effects of SA and A-S and thereby attain the maximum available accuracy of GPS. PPS capable receivers that do not have the proper encryption keys installed will be subject to the accuracy degradations of SA and will be unable to track the Y-code. Maximum GPS accuracy is obtained using the P(Y) code on both L1 and L2. The difference in propagation delay between the two frequencies is used to calculate ionospheric corrections. Some PPS receivers use only the C/A-code. C/A-only receivers must use an ionospheric model to calculate ionospheric corrections since the C/A-code is broadcast only on L1 and dual frequency delay measurements are therefore not available. This will result in less positioning accuracy than with dual frequency P(Y) receivers.

4.3 Standard Positioning Service

The SPS is specified to provide 100 meter (95 %) horizontal positioning accuracy to any GPS user during peacetime. This is approximately equal to 174 m 3-D (95 %). SPS receivers can achieve approximately 360 ns (95 %) UTC time transfer accuracy. The SPS is primarily intended for civilian purposes, although it has many peacetime military uses as well. The SPS horizontal accuracy specification includes the peacetime degradation of SA which is the dominant SPS error source. The A-S feature denies SPS users access to the Y-code. Therefore, the SPS user cannot rely on the P code to measure the propagation delays of L1 and L2 and calculate ionospheric corrections. The C/A code is unaffected by A-S but is broadcast on L1 only. Consequently, the typical SPS receiver uses only the C/A code and must use an ionospheric model to calculate the corrections. This is a less accurate technique than measuring dual frequency propagation delays. The SPS accuracy specification includes this ionospheric modelling error (see table 2).

5. Navigation Using GPS

As explained in paragraph 1, the ranging codes broadcast by the satellites enable a GPS receiver to measure the transit time of the signals and thereby determine the range between a satellite and the user. The navigation data messages enable a receiver to calculate the position of each satellite at the time of transmission of the signal. From this information the user position coordinates and the user clock offset can be calculated using simultaneous equations. Four satellites are normally required to be simultaneously "in view" of the receiver for three-dimensional (3-D) positioning purposes. The following paragraphs give a brief description of the GPS satellite signals and GPS RCVR operation.

5.1 GPS Satellite Signals

P(Y) Code

The P-code is a 267 days long code sequence, and each of the GPS satellites is assigned a unique one week segment of this code. The P-code bit rate is 10.23 MHz and each satellite will have a seven day long portion that restarts every Saturday/Sunday midnight. The P-code will normally be transmitted on both L1 and L2. The P-code is protected against spoofing, (i.e. the deliberate transmissions of incorrect GPS information) by encryption of the P-code. The encrypted P-code is called Y-code. The Y-code can only be accessed by authorized users.

C/A-code

The C/A-code consists of a 1023 bit code with a clock rate of 1.023 MHz; hence it takes only 1 millisecond to run through the whole code. A different C/A-code is assigned to each GPS satellite and is chosen from a set of codes called Gold codes. The C/A-code will normally be transmitted on L1 only. The C/A-code is available to any user of GPS. The C/A-code is used by P-code users to assist the RCVR in reducing the time to acquire the longer P-code. A C/A-code only RCVR is less complex and usually less expensive than a P-code GPS RCVR.

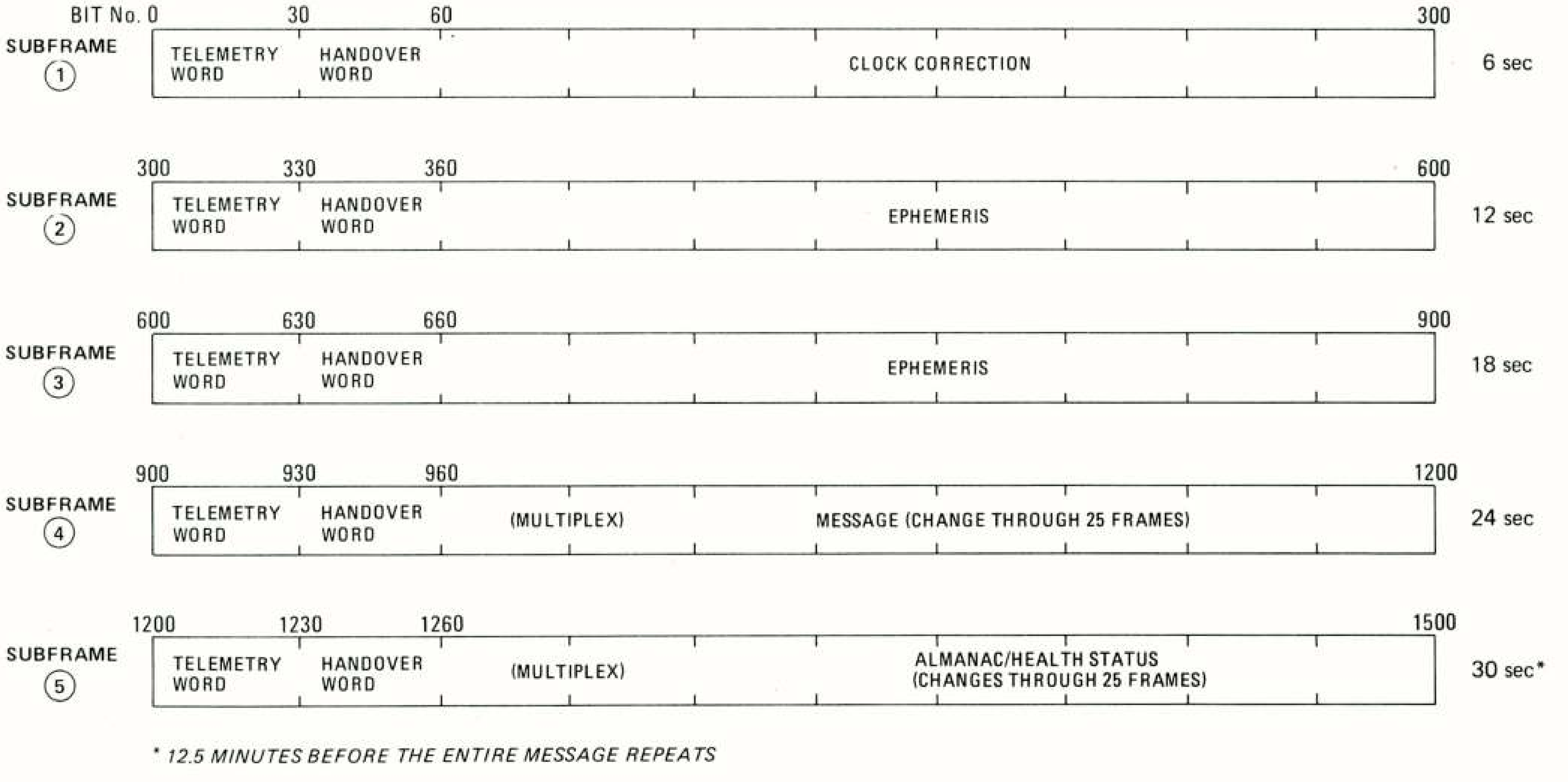


Fig. 8 The content of the navigation message

The Navigation Message

The NAV-msg is superimposed on both the P-code and the C/A-code with a data rate of 50 bits/sec. The NAV-msg contains 25 data frames, each frame consisting of 1500 bits. Each frame is divided into 5 subframes of 300 bits each (see figure 8). It will therefore take 30 seconds to receive one data frame and 12.5 minutes to receive all 25 data frames. Subframes 1, 2 and 3 repeat the same 900 bits of data on all 25 frames. This allows the RCVR to obtain critical NAV-msg data within 30 seconds. The data in the NAV-msg is normally valid for a 4 hour period. The NAV-msg contains GPS system time of transmission; a Hand Over Word (HOW) for the transition from C/A to P-code tracking; ephemeris and clock data for the particular satellite being tracked; and almanac data for all the SVs in the constellation. Additionally, it contains information such as satellite health, coefficients for the ionospheric delay model for C/A-code users, and coefficients to calculate Universal Coordinated Time (UTC).

Satellite Signal Modulation

The GPS satellites use a type of signal modulation called Bi-Phase Shift Keying (BPSK) of the carrier. The BPSK technique reverses the carrier phase when the digital PRN code transitions from 0 to 1 or from 1 to 0 (see figure 9).

The very long sequences of ones and zeros which constitute the C/A- and P-codes are called PRN codes since, to a casual observer, the ones and zeros appear to occur in a random fashion. The resulting frequency spectrum for the carrier, due to the BPSK, equals 20 MHz for the P-code and 2 MHz for the C/A-code (see figure 10). The carrier frequency is suppressed. In actuality, the C/A and P-codes generated are precisely predictable

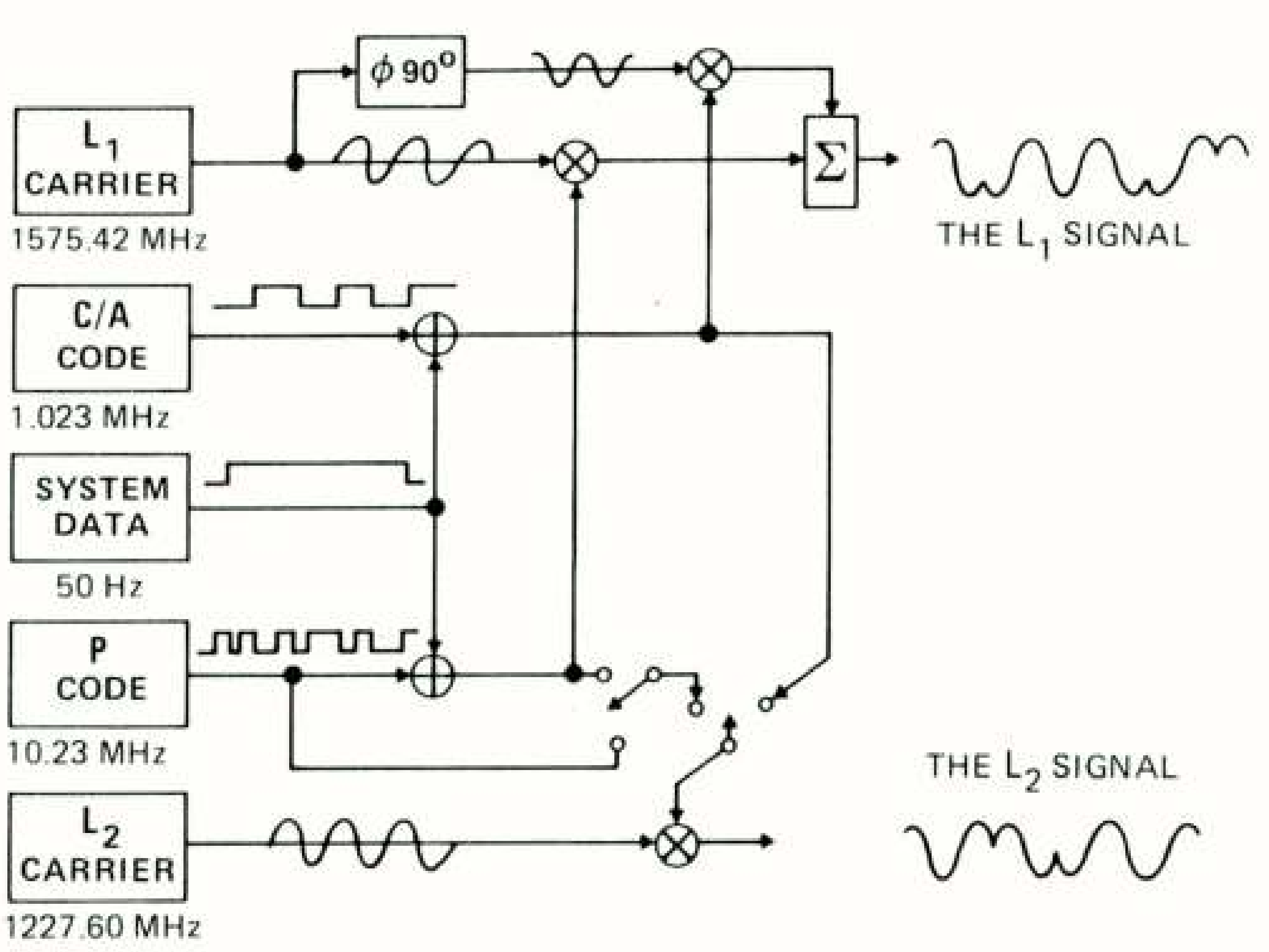


Fig. 9 Modulation of carrier frequencies

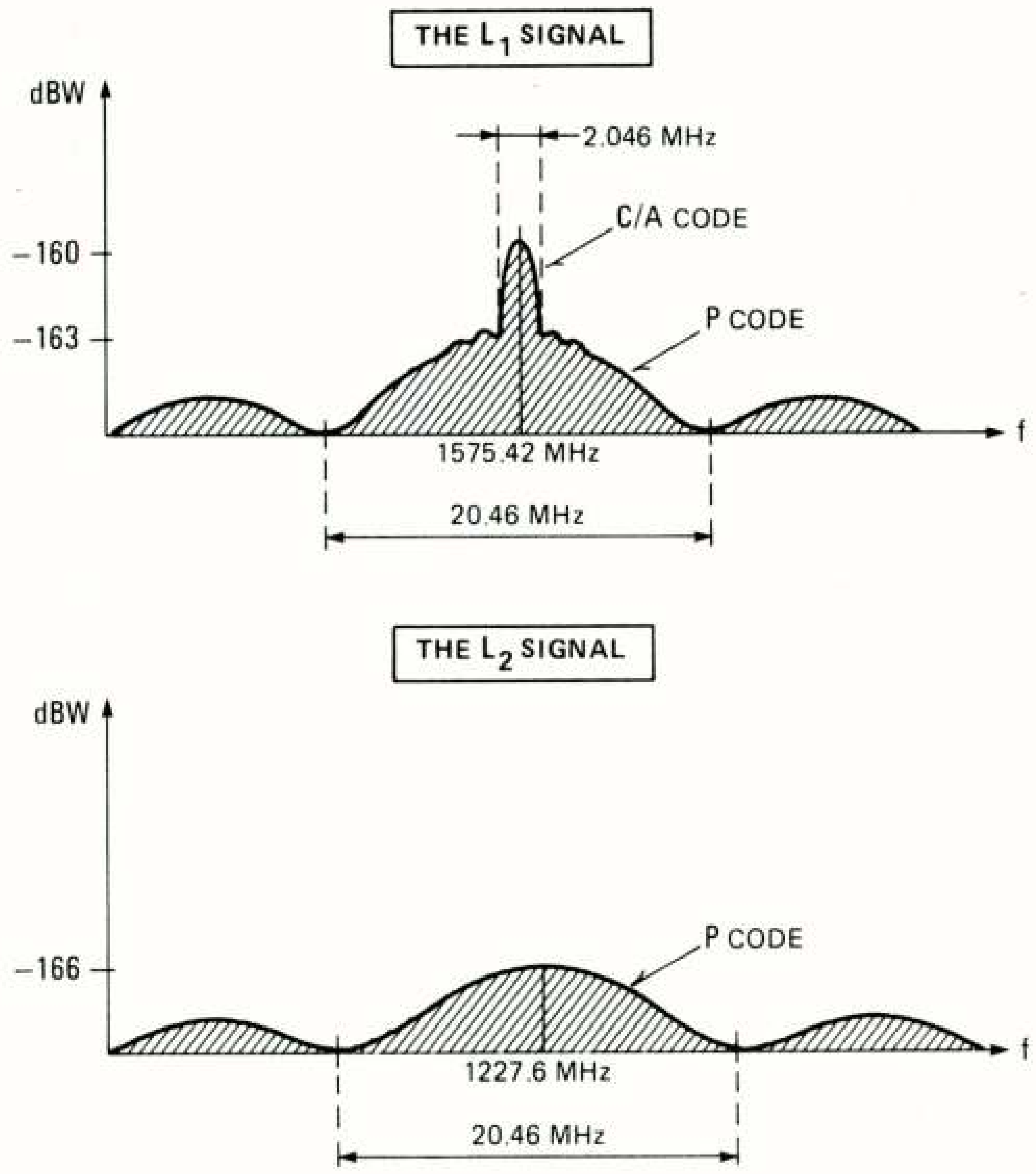


Fig. 10 The spread spectrum signals

relative to the start time of the code sequence. The user can therefore replicate the same code as the satellite. The amount the user must offset his code generator to match the incoming code from the satellite is directly proportional to the range between the GPS RCVR antenna and satellite. Phase shifting of the carrier results in a spreading of carrier power between ± 10.23 MHz of the center frequency due to the P-code BPSK, and ± 1.023 MHz due to the C/A-code BPSK. When the spread spectrum signal is received at the GPS RCVR the signal power is below the thermal noise level. When the satellite signal is multiplied with the GPS RCVR generated P-codes and C/A-codes, the satellite signal will be collapsed into the original carrier frequency band. Signal power is then again concentrated into a very narrow frequency band and becomes well above the thermal noise level.

5.2 Navigation

In order for the GPS RCVR to navigate, it has to acquire and track satellite signals to make pseudorange and deltarange (velocity) measurements, and collect the NAV-msg data. The measurements are termed pseudorange because the clock offset of a GPS RCVR introduces a bias to the true range of the satellite. When the RCVR has acquired the satellite signals form four satellites, achieved carrier and code tracking, and has read the NAV-msg, the GPS RCVR is ready to start navigating.

Figure 11 shows a representative block diagram of a GPS receiver. The GPS RCVR normally updates its pseudorange and relative velocities once every second. The next step is to calculate the GPS RCVR position, RCVR velocity and GPS system time. The GPS RCVR must know GPS system time very accurately, because the satellite signals contain the time-of-transmission from the satellite in GPS time.

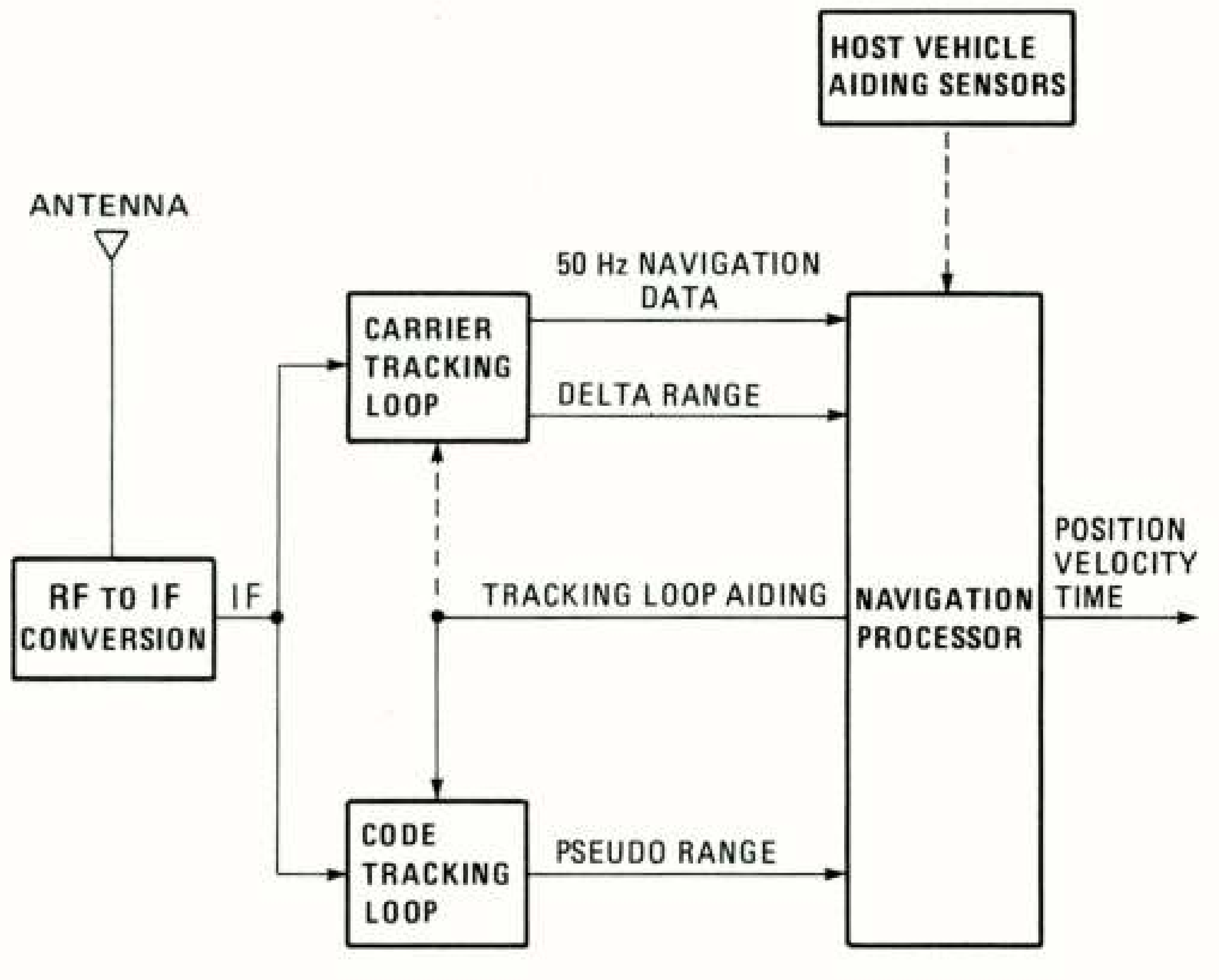


Fig. 11 Block diagram of a typical GPS receiver

Therefore, the GPS RCVR must also use GPS system time as the reference for measuring time-of-arrival of the satellite signals. The difference in time between the signal leaving the satellite and arriving at the GPS RCVR antenna is directly proportional to the range between the satellite and the GPS RCVR, so it is of the utmost importance that the same time reference is used by both the GPS satellites and the GPS RCVR. However, the GPS RCVR is not required to have a high accuracy clock such as an atomic time standard. Instead, a crystal oscillator is used and the GPS RCVR corrects its offset from GPS system time by making four pseudorange measurements as said before. The GPS RCVR can use the four pseudoranges to solve four simultaneous equations with four unknowns. When the four equations are solved, the GPS RCVR has estimates of its position and GPS system time. The GPS RCVR velocity is calculated using the same types of equations, using relative velocities instead of pseudoranges. GPS receivers perform most calculations using an earth-centered earth-fixed coordinate system. They then convert to an earth model defined by the World Geodetic System 1984 (WGS 84). WGS 84 is a very precise model that provides a common grid system for transformations into other coordinate systems or map datums.

6. Conclusion

The GPS system has developed rapidly in the last few years. Ten operational (Block II) satellites have been launched (December 1990) and six Block I SVs are still usable. This constellation provides for a nearly 24-hr, 2-D capability at many places on earth. It may be expected that the system will be fully operational in 1993. For military as well as for civil users then a very accurate 3-D positioning system will be available.

Verantwoording

Bovenstaand artikel is een door de auteur bewerkte versie van het eerste hoofdstuk uit het document ANP-2, "Introduction to Navstar GPS User Equipment", geschreven door het Nato Team, Headquarters Space Systems Division, Los Angeles. Dit hoofdstuk bevat meer informatie dan kon worden gegeven in de voordracht op de NERG werkvergadering op 9 november 1990, terwijl voor wat betreft de status van het systeem de informatie werd aangepast tot 20 december 1990. Gegevens omtrent de nauwkeurigheid van Navstar werden bovendien gehaald uit Draft STANAG 4294, "Navstar GPS System Characteristics". De auteur heeft een relatie met deze twee documenten op grond van het volgende:

In 1977 werd een Memorandum Of Understanding (MOU) ten aanzien van Navstar getekend door de Verenigde Staten enerzijds en negen ander Nato landen, waaronder Nederland, anderzijds. In dit MOU werd ondermeer het volgende geregeld:

- De vestiging van een Nato Team op het Joint Program Office (JPO) in Los Angeles waarvan de leden actief zouden worden ingeschakeld bij de ontwikkeling van het systeem;
- de instelling van een Nato Navstar Steering Committee, om Nato wensen te verwoorden bij het JPO en om het Nato Team te begeleiden.

Het Nato Team in Los Angeles, bestaande uit afgevaardigden van de verschillende landen, werkt sinds die tijd actief mee in de ontwikkeling van het systeem. Auteur dezes was lid van het Team van 1978 tot 1980.

Na een aantal jaren bleek binnen het Nato Steering Committee de behoefte te bestaan aan een ondersteunende groep om zich bezig te houden met de technische aspecten van het Navstar systeem, een leidende rol te spelen bij het opstellen van een Nato STANAG betreffende GPS, informatie uit te wisselen tussen het Nato Team en de deelnemende landen, en het Steering Committee desgevraagd te adviseren bij het nemen van beslissingen. Deze groep staat bekend onder de naam: Nato Navstar Technical Support Group (TSG).

De TSG heeft door zijn activiteiten invloed uitgeoefend op de totstandkoming van STANAG 4294 en ANP-2. Auteur is de afgelopen vijf jaren de vertegenwoordiger voor Nederland geweest in de TSG en fungeert op dit moment als de voorzitter ervan.

Voordracht gehouden tijdens de 383e werkvergadering.

GPSINFO, EEN VIDEOTEX GPS INFORMATIE SYSTEEM

ir. G.M. Lammerts van Bueren
Meetkundige Dienst van Rijkswaterstaat

GPSINFO, a Videotex GPS information system. The Survey Department of Rijkswaterstaat operates an electronic information system with information about the Global Positioning System (GPS). This information system is one way in which the Survey Department performs her task as civil point of contact between GPS-users and the militairy governments. She has acepted this task on NATO request.

De Meetkundige Dienst

De Meetkundige Dienst (MD) is een van de specialistische diensten van Rijkswaterstaat (RWS). De MD is de RWS-dienst voor geo-informatie, geo-informatica en informatica-infrastructuur, op die gebieden waar RWS/V&W haar taak heeft bij het oplossen van maatschappelijke vraagstukken.

De MD levert aan de RWS-diensten geo-informatie in verschillende vormen, waaronder bijvoorbeeld topografische-, thematische-, hoogte- en plaatsinformatie ten behoeve van de voorbereiding en de uitvoering van RWS-taken. De MD is voorts belast met het instandhouden van het nationale net van hoogtegegevens en met het leveren van de waterstaatskaart van Nederland.

Daarnaast adviseert de MD de diverse RWS-diensten, waartoe onderzoek wordt verricht.

In dat kader wordt bij de MD onderzoek verricht naar de toepassingsmogelijkheden van het Global Positioning System (GPS), een nieuw satellietsysteem.
Dit onderzoek is vooral gericht op:

- de landmeetkunde/geodesie;
- de plaatsbepaling en navigatie op zee en in de lucht;
- het personen- en goederenvervoer;
- de fotogrammetrie.

GPS

Het GPS-systeem is een navigatie- en plaatsbepalingssysteem dat ontwikkeld is door het Amerikaanse Ministerie van Defensie. Het verkeert momenteel nog in een opbouw fase, waardoor het aantal satellieten nog beperkt is.

Vanaf 1993 moet het systeem volledig operationeel zijn. Er zullen dan 24 satellieten in een baan om de aarde draaien. Deze satellieten omsluiten de aarde als een soort kooi, zodanig dat er overal op aarde en op ieder tijdstip van de dag minimaal 5 satellieten zichtbaar zijn, met een minimale elevatiehoek van 5 graden. De satellieten zenden continu signalen uit die opgevangen worden door een speciale ontvanger. Uit de looptijd van de signalen kan de afstand naar de satellieten berekend worden.

Uit de vier gemeten afstanden is zeer nauwkeurig de positie op of boven de aarde te berekenen.

Hoewel GPS een militair systeem is, kunnen civiele gebruikers het kosteloos gebruiken.

Met name voor de scheep- en luchtvaart is het GPS-systeem als navigatiemiddel zeer interessant vanwege zijn wereldwijde dekking en nauwkeurigheid. Ook voor het personen- en goederenvervoer biedt GPS een groot aantal mogelijkheden.

Plaats en snelheid kunnen met behulp van GPS bepaald worden, waardoor route-begeleiding mogelijk is. Als landmeetkundig instrument heeft het GPS-systeem een aantal voordelen ten opzichte van de klassieke manier van landmeten.

Met GPS kunnen snel, eenvoudig en zeer nauwkeurig punten in het terrein ten opzichte van elkaar gemeten worden zonder dat deze onderling zichtbaar zijn. De metingen kunnen in principe onder alle weersomstandigheden worden uitgevoerd.

Achtergrond van GPSINFO

In samenhang met de advies-/onderzoekstaak binnen RWS-/V&W heeft de MD in NATO verband de taak op zich genomen om te fungeren als civiele vertegenwoordiger voor de militairen op het gebied van informatie m.b.t. het GPS plaatsbepalings systeem.

De MD vervult hiermee een intermediaire functie tussen enerzijds de Amerikaanse overheid, als exploitant van het GPS plaatsbepalingssysteem, en anderzijds de gebruikers in Nederland. Zij heeft deze taak naar zich toe getrokken omdat zij de kwaliteit van de informatie kan waarborgen, voor eigen gebruik en voor derden, zonder commerciële belangen.

Dit houdt in dat de MD (potentiële) gebruikers in Nederland informeert over de mogelijke toepassingen van het GPS-systeem, de kwaliteit van het signaal en de plannen van de Amerikaanse overheid m.b.t. de toekomst van GPS.

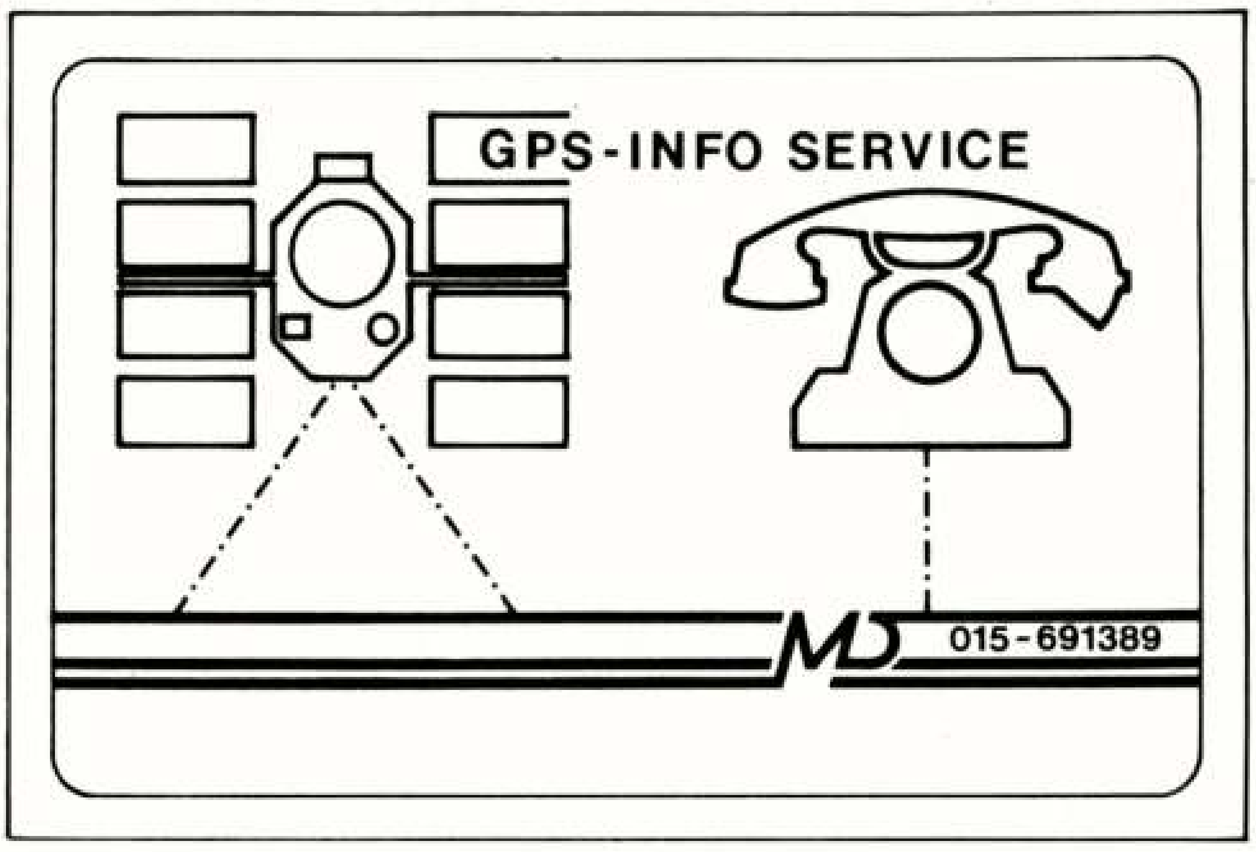
Daarnaast kunnen de gebruikers van GPS eveneens hun wensen, aanmerkingen en vragen m.b.t. het GPS-systeem via de MD kenbaar maken.

De intermediaire functie van de MD is in de volgende twee delen op te splitsen:

1) De adviesfunctie die de MD, middels haar lidmaatschap van het CGSSC (Civil GPS Service Steering Committee, het Amerikaanse overlegorgaan voor civiel gebruik van GPS), gestalte geeft.
   Het CGSSC komt vier maal per jaar in Amerika bijeen.
2) Het videotex informatiesysteem, GPSINFO, waar gebruikers langs geautomatiseerde weg informatie over de status en de achtergrond van GPS kunnen opvragen, en kunnen communiceren met de systeembeheerder en met elkaar.

In de verdere uitleg wordt enkel ingegaan op de functie van het videotex informatie systeem GPSINFO.

Survey department



Doelgroep

GPS gebruikers kunnen het systeem het meest zinvol gebruiken indien ze over goede en recente informatie beschikken over de status van het GPS systeem. Zeker tijdens de periode dat GPS nog niet volledig operationeel verklaard is.

In deze periode zal GPS namelijk niet 24 uur per dag beschikbaar zijn. Dit is omdat nog niet alle satellieten in hun baan zijn gebracht en omdat er nog geregeld proeven met de satellieten worden gehouden waardoor sommige satellieten voor enige tijd niet of minder bruikbaar zijn.

De doelgroep van GPSINFO bestaat uit huidige en toekomstige GPS- gebruikers in Nederland die behoefte hebben aan status en achtergrond informatie. Meer concreet zijn dit die mensen of bedrijven die gedurende een bepaalde periode continue GPS-dekking nodig hebben, of dit nu t.b.v. navigatie, survey of puntsbepaling is.

Een beperking van GPSINFO is dat het geen realtime informatie geeft en dus niet te gebruiken is als integrity monitor. Toch is de status informatie over GPS zinvol voor navigatietoepassingen om te weten of het systeem op een bepaalde dag volgens planning naar behoren te gebruiken is. Niet geplande uitval van satellieten is in principe de enige tegenslag waar men dan nog mee te maken kan krijgen.

GPSINFO is het meest zinvol te gebruiken voor de planning van survey en puntsbepalings toepassingen. Hierbij kunnen namelijk veel manuren verloren gaan indien men niet op de hoogte is van de meest recente gegevens van het satelliet systeem.

Wijze van informatieverstrekking

GPSINFO is een electronisch BB (Bulletin Board) waarbij het videotex protocol gehanteerd wordt. Op dit BB worden recente gebeurtenissen op het gebied van GPS vermeld, en is achtergrondinformatie over het GPS systeem te raadplegen.

GPSINFO bevat informatie uit de volgende bronnen:

- Het officiële Amerikaanse bulletin board voor civiele GPS gebruikers, geëxploiteerd door de USCG (United States Coast Guard).
- Een meer algemeen gericht bulletin board, waar ook informatie over tijd en Loran-C te raadplegen is, geëxploiteerd door de USNO (United States Naval Observatory).
- Bulletin boards van andere GPS informatie centra (momenteel alleen Noorwegen en Engeland).
- Informatie die naar buiten wordt gebracht tijdens bijeenkomsten van het CGSSC.
- Informatie die via de GPS ontvangers van de MD wordt verkregen.
- Informatie van derden.

Deze informatie wordt, voor zover redelijkerwijs mogelijk, langs electronische weg gearchiveerd (computerbestand) en zoveel mogelijk via GPSINFO ter beschikking van belangstellenden gesteld. Door deze wijze van beschikbaar stellen is de informatie 24 uur per dag te raadplegen.

Vanwege de keuze voor videotex, is het gebruik van het systeem bijzonder eenvoudig.

Om GPSINFO te kunnen gebruiken moet men beschikken over een toegangsnummer voor het systeem, alsmede een password. Op verzoek wordt dit aan de iedere gebruiker verstrekt. Om de toegang tot het systeem te kunnen realiseren moet men beschikken over minimaal de volgende hardware:

- een XT-computer;
- een E.G.A kleurenscherm;
- een 1200/1200 modem.

Daarnaast moet men een communicatie pakket gebruiken dat in staat is om met een videotex database te communiceren en dat behalve de standaard Prestel eigenschappen ook nog in staat moet zijn om 80 koloms pagina's

weer te geven en om file transfer download uit te voeren, zoals:

- Supertel versie 3.21E;
- Telstar prive;
- Telstar ansi.

De Meetkundige Dienst verleent deze service momenteel kosteloos.

Beschikbare informatie

De abonnees van GPSINFO kunnen informatie opvragen over:

- Het laatste nieuws:
  Informatie over tests, lanceringen en onderhoud van de satellieten, die invloed hebben op de werkzaamheden van de gebruikers. Deze informatie wordt dagelijks geactualiseerd.
- Positie gegevens:
  Wekelijks worden nieuwe almanac gegevens van alle GPS satellieten in het systeem ingevoerd. De gegevens zijn vervolgens per individuele satelliet te raadplegen.
- Status gegevens:
  Via een submenu zijn gegevens over: de GPS constellatie en de lanceerdatum, gezondheid en kloktype van de individuele GPS satellieten te raadplegen. Bij de satellietstatus wordt ook recente en nabije uitval van satellieten weergegeven.
- Historische gegevens:
  Bij deze keuze krijgt men, na ingave van een datum, een overzicht van de eerste 8 NANU's (Notice Advisories to Navstar Users, ofwel waarschuwingen voor GPS gebruikers) die op of na die datum zijn uitgegeven.
  Hiermee wordt het voor een gebruiker mogelijk om achteraf te zien of moeilijkheden met zijn metingen misschien verklaarbaar zijn door het slecht functioneren van een of meer satellieten, waarvan hij vooraf niet op de hoogte was.
- Verzoeken:
  Het is voor de gebruiker mogelijk om een aanvraag voor een voorspelling van satellietbeschikbaarheid voor een bepaalde datum en tijd aan te vragen. Ook kan de gebruiker een willekeurige vraag of boodschap naar de systeembeheerder sturen.
  Het is sinds begin januari 1991 ook mogelijk om file's met almanac gegevens te sponzen (downloaden) via GPSINFO. Hierdoor kunnen gebruikers zonder eigen GPS-ontvangers maar met een eigen voorspellingsprograamma ook beschikken over de nieuwste baangegevens van de satellieten.
- Systeem informatie:
  Via deze keuze komt men in een submenu met informatie over het GPS systeem. Voorbeelden hiervan zijn: lanceerschema, politiek, en te behalen precisie.
- Algemene informatie:
  Via deze keuze kan men vervolgens overzichten van ontvangers, gebruikers, projecten, literatuur en bijeenkomsten raadplegen. Deze informatie is momenteel nog maar voor een beperkt deel beschikbaar.
- Transformatie's:
  Er wordt gewerkt aan het implementeren van de mogelijkheid van het uitvoeren van een aantal transformatie's op coördinaten.
- Mailbox:
  Via het submenu van de mailbox is vrijelijk MAIL te versturen aan alle gebruikers van GPSINFO. Er is een optie aanwezig om een overzicht te krijgen van alle aanwezige gebruikers. Tevens kan men ontvangen MAIL via dit submenu raadplegen.

Hiernaast is het de gebruiker uiteraard toegestaan om het aan hem toegekende password te wijzigen.

De nadruk in de uitbreiding van het huidige prototype ligt op het weergeven van gedeelten van interessante GPS-documenten, het verbeteren van de overzichten en het implementeren van de mogelijkheid van coördinaat transformatie's.

Voordracht gehouden tijdens de 383e werkvergadering.

NEDERLANDS ELEKTRONICA- EN RADIOGENOOTSCHAP
THE INSTITITION OF ELECTRICAL AND ELECTRONICS ENGINEERS
BENELUX SECTION
384e werkvergadering



PROF. DR. IR.
P. C. T. VAN DER LAAN

UITNODIGING

voor de lezingendag op **woensdag 12 december 1990,** in het **Philips Natuurkundig Laboratorium, Prof Holstlaan, Eindhoven.**
Thema: ELECTRO-MAGNETISCHE COMPATIBILITEIT (EMC).

PROGRAMMA:

09.30 - 10.00 uur: Ontvangst, koffie

10.00 - 10.05 uur: Inleidend overzicht door dagvoorzitter

10.05 - 10.25 uur: EMC, OOK VOOR INTENSE STORINGEN;
PROF. DR. IR. P. C. T. VAN DER LAAN, TUE, Eindhoven

10.25 - 10.45 uur: EMC-KWALITEIT VAN HET ELEKTRICITEITSNET;
IR. G. BLOM, KEMA, Arnhem

10.45 - 11.05 uur: EMC VAN ISDN-APPARATUUR;
IR. W. PASMOOIJ, PTT Research, Leidschendam

11.05 - 11.25 uur: Koffie-Pauze

11.25 - 11.45 uur: EMC-ASPECTEN VAN MODERNE DIGITALE SCHAKELINGEN EN DEVICES;
ING. L. P. JANSSEN, Philips Nat. Lab., Eindhoven

11.45 - 12.05 uur: EMC-ASPECTEN VAN AUTOMOTIVE ELECTRONICS;
ING. R. VAN NULAND, Volvo Car, Helmond

12.05 - 13.45 uur: Lunch-Pauze

13.45 - 14.05 uur: HIGH INTENSITY RADIATED FIELDS BY AIRCRAFT;
IR. S. H. A. PETERS, NLR, Emmeloord

14.05 - 14.25 uur: EMC-ASPECTEN VAN RADIO-ASTRONOMIE;
IR. T. A. TH. SPOELSTRA, Radio Sterrenwacht, Dwingeloo

14.25 - 14.45 uur: ONDERWIJS EN EMC;
DR. J. J. GOEDBLOED, Philips Nat. Lab., Eindhoven

14.45 - 15.05 uur: Thee-Pauze

15.05 - 15.25 uur: STAND VAN ZAKEN EMC-RICHTLIJN EG;
IR. M. VROLIJK, Philips Concern Stand., Eindhoven

15.25 - 15.45 uur: IMPLEMENTATIE EMC-RICHTLIJN EG;
ING. C. L. NIJDAM, HDTP Verkeer en Waterstaat, Groningen

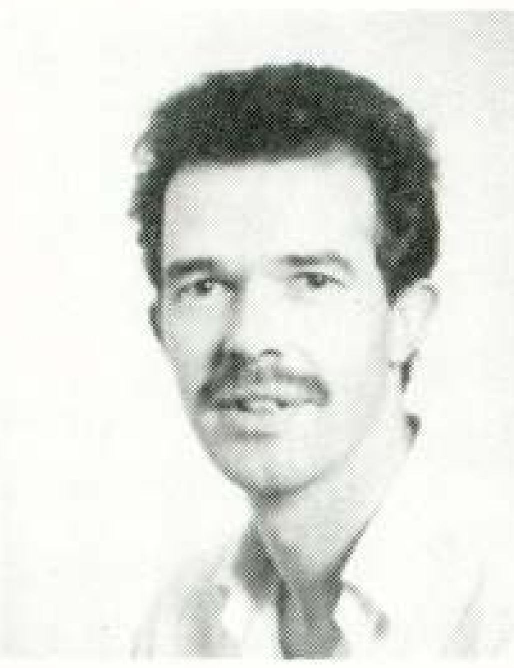
15.45 - 16.15 uur: BEANTWOORDING VRAGEN EMC-RICHTLIJNEN;
Panel met o.m.: **IR. VROLIJK, ING. NIJDAM EN IR. PASMOOIJ**

Leidschendam, november 1990.

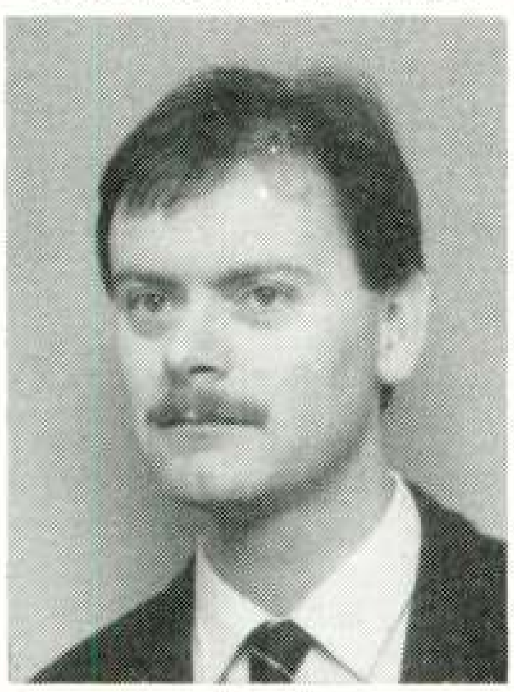
Namens de samenwerkende verenigingen,
Ir. N. H. G. Baken.
Tel. 070 - 332 64 82



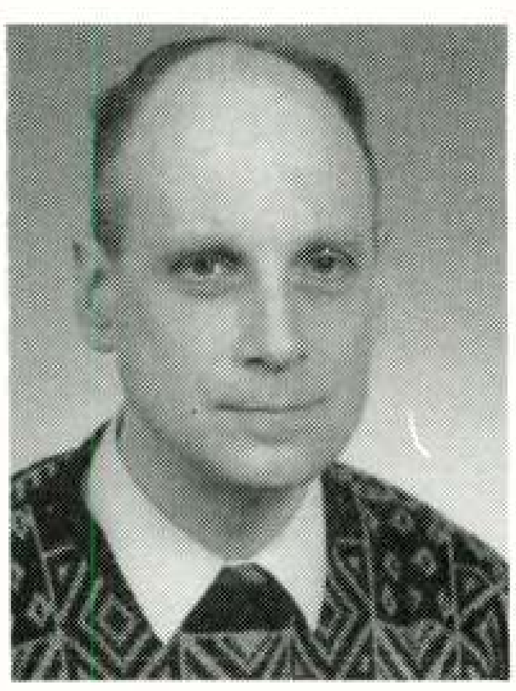
IR. W. PASMOOIJ



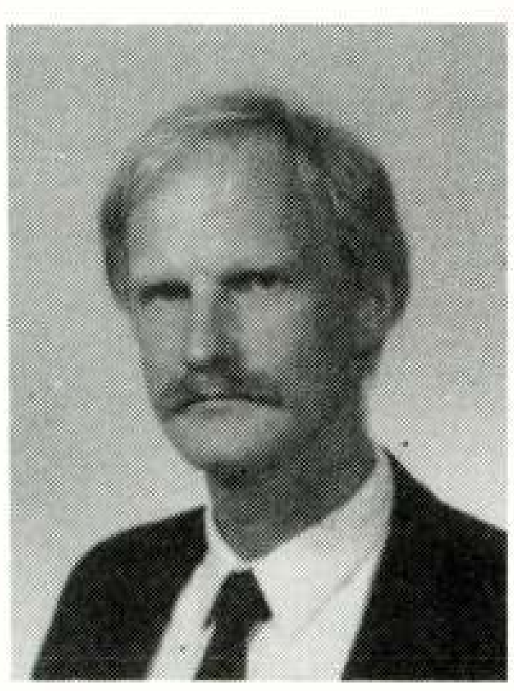
ING. L. P. JANSSEN



IR. S. H. A. PETERS



IR. T. A. TH. SPOELSTRA



ING. C. L. NIJDAM

DE EMC-KWALITEIT VAN HET ELEKTRICITEITSNET

Ir. G. Blom
NV KEMA

This article, which deals with the EMC quality of the electricity transmission networks in the Netherlands, briefly reviews the types of voltage distortion that can be distinguished as well as their causes and consequences; furthermore, it contains a discussion of the degree of occurance of voltage distortion, it outlines emission and immunity requirements and describes the way in which the Dutch electricity supply undertakings monitor the level of voltage distortion.

Inleiding

Er valt een toenemende belangstelling te bespeuren voor het verschijnsel netspanningsvervorming, of kortweg netvervuiling. Enerzijds komt dit, omdat door de opkomst van de vermogenselektronica (voor het regelen van elektrische machines en toestellen) de mate waarin netvervuiling optreedt een stijgende tendens vertoont, en anderzijds omdat er door de voortgaande ontwikkelingen in met name de micro-elektronica steeds meer apparatuur op de markt komt, waarvan de goede werking ongunstig door netvervuiling kan worden beïnvloed als er in de ontwerpfase van die apparatuur al geen speciale maatregelen worden genomen.

Er zal zonder al te veel in detail te treden op de volgende zaken worden ingegaan:

- de verschillende soorten netvervuiling die onderscheiden kunnen worden, de oorzaken en de mogelijke gevolgen ervan
- de mate waarin de verschillende soorten netvervuiling in de Nederlandse elektriciteitsnetten optreden
- de eisen die met betrekking tot de emissie van netvervuiling worden gesteld aan de op het openbare elektriciteitsnet aan te sluiten toestellen
- de eisen die met betrekking tot immuniteit voor netvervuiling worden gesteld aan op het openbare elektriciteitsnet aan te sluiten apparatuur
- de bewaking van het netvervuilingsniveau door de Nederlandse elektriciteitsbedrijven.

Soorten netvervuiling, de oorzaken en mogelijke gevolgen

Naar soort is netvervuiling globaal in 3 groepen in te delen:

- kortstondig optredende stoorspanningen, de zogenaamde transiënts. Het betreft verschijnselen met een duur van enkele tientallen nanoseconden (of zelfs korter) tot enkele milliseconden. Een spike is een bijzondere vorm van een transiënt: een kortstondige spanningspiek

- spanningsfluctuaties, met als bijzondere verschijnselen spanningdalingen van korte duur, de zogenaamde spanningsdips. Spanningsfluctuaties zijn variaties in de effectieve waarde van de netspanning, die een maximale frequentie van de helft van de netspanningsfrequentie kunnen hebben. Zoals gezegd is een spanningsdip een bijzonder geval van een spanningsfluctuatie; het is een spanningsverlaging van tenminste 10% die tussen 10 ms en 60 s duurt

- (hogere) harmonischen, subharmonischen, interharmonischen e.d. Interharmonischen zijn periodieke verschijnselen met een frequentie gelegen tussen twee harmonischen.

In de volgende figuren zijn voorbeelden gegeven van verschillende soorten netvervuiling.

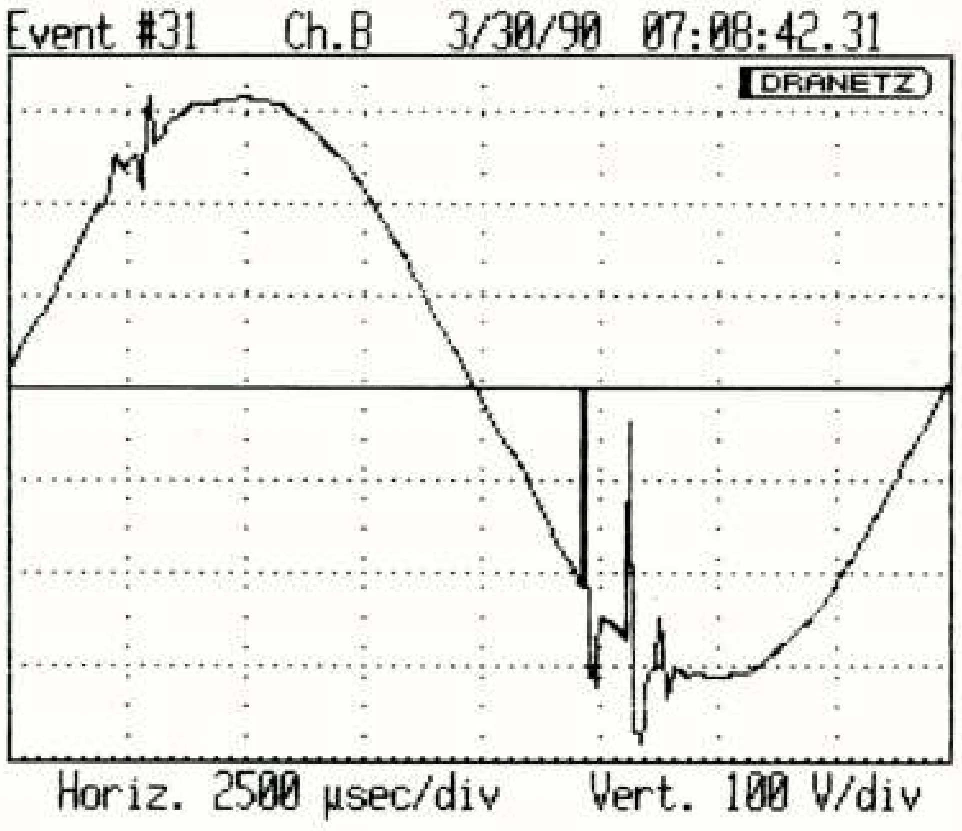


Fig. 1: Netvervuiling door transients

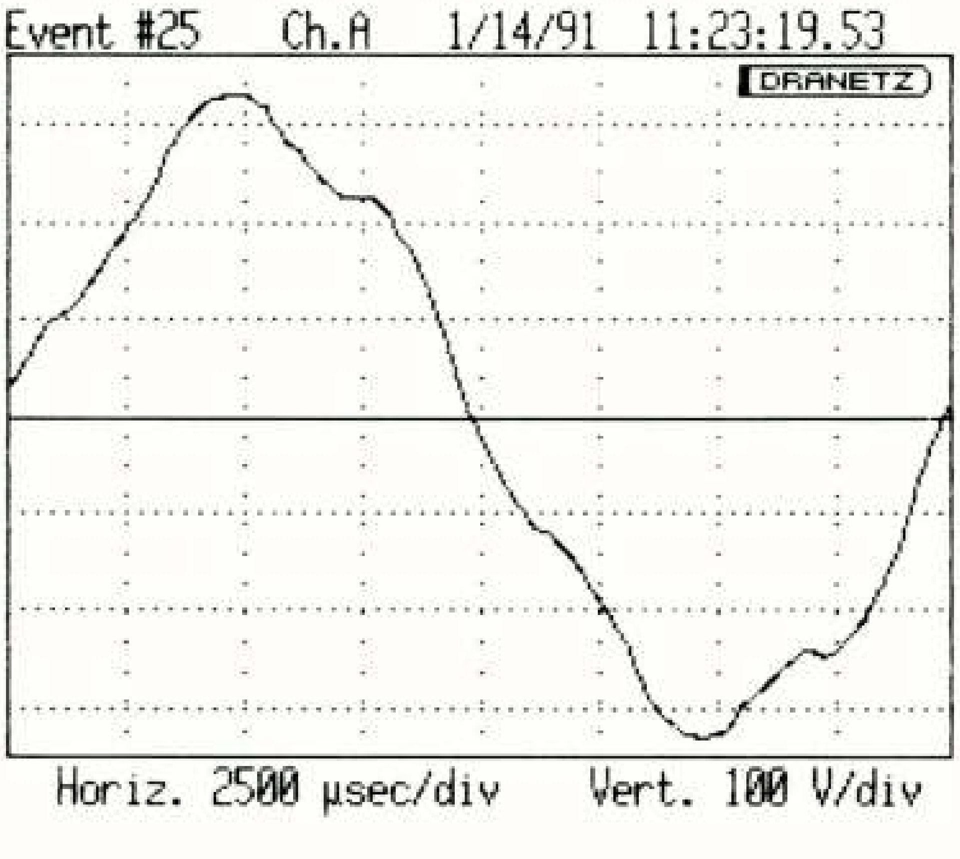


Fig. 2: Netvervuiling door 5^{e} harmonische

Deze soorten netvervuiling kunnen afzonderlijk of in combinatie optreden en worden veroorzaakt door:

- blikseminslag (dit kan transiënts in een elektriciteitsnet veroorzaken)
- het aanspreken van smeltveiligheden (transiënts)
- al of niet gestuurde gelijkrichters en andere convertors, spannings-frequentieregelingen, chopperschakelingen e.d. (harmonischen, subharmonischen, interharmonischen, transiënts in de vorm van commutatietrillingen)
- het inschakelen van grote vermogens en van grote inductieve en capacitieve belastingen (spanningsfluctuaties, transiënts)
- storingen in hoog-, midden- en laagspanningsnetten (dips en spanningsonderbrekingen, qua tijd variërend van kortstondig tot langdurig).

Gevolgen van het optreden van netvervuiling kunnen zijn:

- extra warmte-ontwikkeling (veroorzaakt door harmonischen etc.) in elektrische machines (elektromotoren en generatoren), transformatoren en condensatoren eventueel gevolgd door het aanspreken van de desbetreffende beveiligingen (voor zover aanwezig) of zelfs beschadiging van deze componenten
- tijdelijke verstoring van de goede werking en beschadiging van elektronische apparatuur zoals PC's (transiënts, dips, maar ook: interharmonischen)
- lichtflikkeringen veroorzaakt door lampen aangesloten op het elektriciteitsnet (spanningsfluctuaties)
- het verstoren van de goede werking van toonfrequent-afstandsbesturingssystemen, zoals die onder meer door de elektriciteitsbedrijven worden gebruikt voor het op afstand in- en uitschakelen van belastingen, het omschakelen van dubbeltarief-telwerken van kWh-meters etc. (harmonischen, interharmonischen).

Het optreden van netvervuiling in de Nederlandse elektriciteitsnetten

Transiënts zijn in termen van het elektriciteitsnet hoogfrequent verschijnselen. De propagatie ervan is ten gevolge van de grote demping van het elektriciteitsnet voor deze verschijnselen, beperkt tot de installatie van de verbruiker die transiënts veroorzaakt en zijn onmiddellijke omgeving. Bij metingen verricht door KEMA bij verbruikers die klaagden over regelmatig optredende storing aan

(digitale) elektronische apparatuur, werd geen enkele keer een transiënt vastgelegd waarvan de topwaarde groter was dan het testniveau waarvoor de betreffende apparatuur nog immuun zou moeten zijn volgens de van toepassing zijnde IEC-normen, zoals IEC 255 en 801. De maximale waarden van de verschijnselen die werden geregistreerd, lagen in de orde van grootte van 300 tot 400 V. In praktisch alle gevallen kon een andere oorzaak van de storing worden aangewezen:

- fouten bij het installeren, zoals geen of een gebrekkige aarding
- in één geval: een plaatselijk (te) hoge TF-spanning
- het niet voldoen van de gestoorde apparatuur aan de minimaal te stellen eisen voor wat betreft de immuniteit voor netvervuiling.

Hinder ten gevolge van netspanningsfluctuaties komt in Nederland nauwelijks voor. Ook hiervan kan worden gezegd, dat als het optreedt het veelal beperkt is tot de (in dit soort gevallen te licht ontworpen) installatie van de verbruiker die de hinder veroorzaakt en de onmiddellijke omgeving. In landen met industriële installaties die het net sterk fluctuerend belasten, zoals bijvoorbeeld het geval kan zijn bij elektrische lichtboogovens, vormen spanningsfluctuaties een veel wijdverbreider probleem.

Netvervuiling in de vorm van harmonische componenten dreigen een niet te onderschatten probleem te gaan worden. Dat komt door:

- de doorgaans geringe verzwakking van dit soort componenten in het elektriciteitsnet. Dat geldt niet voor homopolaire harmonische componenten; deze worden niet door een distributie- of vermogenstransformator met een driehoekswikkeling doorgegeven
- de gestage groei van het aantal niet-lineaire belastingen en de cumulatie van de door ieder van deze belastingen afzonderlijk veroorzaakte harmonischen
- de grote kans op het optreden van resonantieverschijnselen in een net.

Als er geen maatregelen worden genomen, mag worden verwacht, dat de grootte van verschillende harmonischen in de spanning van de elektriciteitsnetten binnen afzienbare tijd regelmatig op te veel plaatsen en te lang de voor dit soort netvervuiling geldende "compatability levels" zal overschrijden. Dat is dan ook de reden, dat een groot aantal Nederlandse elektriciteitsbedrijven zijn begonnen met het bewaken van het harmonischenniveau in hun netten.

Op de wijze waarop dat gebeurt, zal hierna nog worden ingegaan.

<u>Emissie-eisen</u>

Met uitzondering van transiënts, wordt er voor wat betreft de emissie van de andere hiervoor genoemde soorten netvervuiling wel eisen gesteld. Dat geldt met name voor de emissie van netvervuiling door bepaalde op het laagspanningsnet aan te sluiten toestellen, zoals huishoudelijke apparatuur. Deze eisen zijn te vinden in IEC-publikatie 555, waarvan deel 2 betrekking heeft op door deze toestellen veroorzaakte harmonischen en deel 3 op spanningsfluctuaties.

Er wordt op dit moment gewerkt aan een complete wijziging van deze norm, waarbij onder meer voor wat betreft de hoogte van de eisen onderscheid wordt gemaakt tussen verschillende categorieën toestellen en waarbij bovendien het toepassingsgebied zal worden uitgebreid tot vrijwel alle op het laagspanningsnet aan te sluiten toestellen. Verder zullen de toe te passen meetmethodes worden aangegeven en zullen er eisen in worden opgenomen waaraan de toe te passen meetinstrumenten moeten voldoen. Ook zullen er eisen worden geformuleerd voor de maximaal te veroorzaken grootte van interharmonischen.

Voor industriële toestellen en installaties zijn in internationaal verband geen eisen geformuleerd. In veel landen - zoals in Nederland - zijn hiervoor door de nationale elektriciteitsbedrijven eisen gesteld, waarnaar veelal wordt verwezen in de aansluitvoorwaarden. Deze eisen hebben betrekking op harmonischen en soms ook op spanningsfluctuaties.

<u>Immuniteitseisen</u>

Immuniteitseisen met betrekking tot verschillende soorten netvervuiling zijn ondergebracht in verschillende normen, zoals de IEC-publikaties 255 en 801 en EEC-directive No. C 42/9.

KEMA gaat bij het beproeven van apparatuur op immuniteit voor netvervuiling uit van deze normen. Het gaat daarbij om:

- beproevingen met stoorspanningen
- diëlektrische beproevingen
- elektrostatische ontladingstests
- beproevingen met voedingsspanningsvariaties.

Verder wordt er uiteraard ook beproefd op immuniteit voor elektromagnetische velden.

Afhankelijk van het toepassingsgebied en de omgeving waar de te beproeven apparatuur zal worden geïnstalleerd, varieert de hoogte

van de immuniteitseisen.

Er worden drie klassen onderscheiden:
- klasse III: apparatuur opgesteld in een industriële omgeving of gekoppeld aan hoogspanningsinstallaties (voorbeelden: apparatuur toe te passen in ruimtes waar industriële procesinstallaties staan opgesteld, in elektriciteitscentrales, in hoogspanningsstation etc.)
- klasse II : apparatuur opgesteld in een niet-industriële omgeving en niet gekoppeld aan hoogspanningsinstallaties (voorbeelden: apparatuur toe te passen in bedieningsruimtes van de procesindustrie, in laboratoriumruimtes etc.)
- klasse I : apparatuur waaraan geen bijzondere eisen worden gesteld.

Eisen met betrekking tot immuniteit voor harmonische spanningen zijn onder meer opgenomen in produktnormen zoals:
- CENELEC-document HD 434 en IEC International Standard 1037, die beiden betrekking hebben op toonfrequent-ontvangers toe te passen in afstandsbesturingssystemen
- IEC-publikatie 687 en IEC International Standard 1036, die betrekking hebben op elektronische kWh-meters
- NEN 3173 ("Roterende elektrische machines")
- VDE 0160 ("Bestimmungen für die Ausrustung von Stark-stromanlagen mit elektronische Betriebsmitteln").

<u>De bewaking van het netvervuilingsniveau door de Nederlandse elektriciteitsbedrijven.</u>

Door een groot deel van de Nederlandse elektriciteits-bedrijven wordt meegewerkt aan een systeem waarbij steekproefsgewijs de hoogte van de harmonische componenten in de netspanning wordt bewaakt. Daartoe zijn grenzen vastgelegd bij overschrijding waarvan door het desbetreffende elektriciteitsbedrijf maatregelen zullen worden genomen. Voor bijvoorbeeld de 5e harmonische is dit 5% en voor de 11e 3%. Deze zogenaamde actiegrenzen zullen op korte termijn worden aangepast aan de compatibility-levels voor harmonischen vermeld in IEC International Standard 1000-2-2, welke in mei 1990 is gepubliceerd. Deze aanpassing houdt in, dat onder meer het actieniveau voor de 5e harmonische zal worden verhoogd tot 6% en die voor de 11e harmonische tot 3,5%. Het bij de bewaking gehanteerde criterium is, dat op niet meer dan 10% van de plaatsen in het elektriciteitsnet genoemde grenzen langer dan 1% van de tijd mogen worden overschreden.

De controle of aan dit criterium wordt voldaan, vindt plaats door middel van een steekproef berustend op attributencontrole, waarbij per jaar op 40 aselect gekozen plaatsen in het LS-net gedurende één maand wordt gemeten.

Met dit bewakingssysteem is in 1989 gestart. Voorafgaande daaraan en parallel ermee zijn door de elektriciteitsbedrijven op een groot aantal plaatsen (269) in middenspanningsnetten metingen verricht om een indruk te krijgen van de mate van netvervuiling in deze netten en om netten met veel netvervuiling te traceren. Deze metingen werden in alle gevallen verricht aan de secundaire zijde van de vermogenstransformatoren. Het resultaat ervan kan kort samengevat als volgt worden weergegeven:
- op 2 van de 269 plaatsen (=0,75%) werd geconstateerd, dat de voor de 5e harmonische gestelde actiegrens (=5%) langer dan 1% van de tijd werd overschreden
- wat betreft de 11e harmonische (waarvoor een actiegrens van 3% geldt) was dit het geval voor 6 van de 269 plaatsen (=2,25%).

Behalve aan harmonische componenten, zijn er in Nederland door een aantal elektriciteitsbedrijven en geïnitieerd door de Unipede-werkgroep DISDIP ook metingen uitgevoerd bedoeld om spanningsdips vast te leggen. Uit de resultaten kan voor wat betreft Nederland worden geconcludeerd, dat er op enige plaats in de laag- en middenspanningsnetten gemiddeld 4 keer per jaar een spanningsdip optreedt.

Behalve door Nederlandse elektriciteitsbedrijven werd er aan deze metingen ook meegewerkt door elektriciteitsbedrijven in Noorwegen, Italië, Oostenrijk, Engeland en het voormalige West-Duitsland. Er werden in totaal 5021 spanningsdips geregistreerd. Deze kunnen worden geclassificeerd naar duur en grootte zoals is aangegeven in de volgende tabel.

Tabel

Percentages (van 5021 gemeten) dips
geclassificeerd naar duur en grootte

Duur ->	10 ms - 100 ms	.100 ms - 500ms	500 ms - 1s	1 s - 3 s	3 s - 20 s	20 s - 1min.
Grootte:						
10 < 30%	29,0	26,5	2,9	1,4	0,3	0,0
30 < 60%	3,2	14,4	1,2	0,2	0,0	0,0
60 <100%	0,3	5,4	1,0	0,2	0,1	0,0
100%	0,2	2,8	6,6	0,9	1,0	2,4

Voordracht gehouden tijdens de 384e werkvergadering.

EMC-eisen voor apparatuur met ISDN S- en T-interface

ir. W.A. Pasmooij
PTT Research, Leidschendam

EMC requirements for equipment with ISDN S- and T-interface. The introduction of ISDN demands for dedicated EMC-requirements in which special tests are specified for both emission and immunity aspects of the S- and T-interface. This paper summarizes ISDN-related requirements that have recently been proposed by CISPR G WG2 and ETSI EE4.

1 Mogelijkheden met ISDN

De afkorting ISDN staat voor: *'Integrated Services Digital Network'*. Dat wil zeggen dat meer telecommunicatiediensten (spraak, data, tekst, beelden) via één universeel digitaal netwerk aangeboden worden. In de toekomst zal ook op abonneeniveau gebruik gemaakt worden van glasvezels waardoor de transportcapaciteit enorm zal zijn; hetzelfde kan echter gezegd worden van de investeringen die ermee gemoeid zijn. Op korte termijn is het daarom economisch interessant om gebruik te blijven maken van reeds geïnstalleerde symmetrische koperparen, door sommigen wel eens oneerbiedig aangeduid met 'smalband ISDN'.
Toch zijn de voordelen die het gedigitaliseerde net een gebruiker biedt groot in vergelijking met de huidige situatie.
Zo is het volgende onder meer mogelijk:

- Gericht bellen naar één van de maximaal 8 op de busstructuur aan te sluiten randapparaten.
- Faxen met hoge snelheid.
- Twee apparaten gelijktijdig betrekken in een verbinding. Tijdens een telefoongesprek kan bijvoorbeeld data overgezonden worden zonder het gesprek te hoeven verbreken..
- Efficiënt transport van computerdata zonder een invoice-band modem als vertragende factor.
- PC met behulp van plug-in card ombouwen tot dedicated ISDN-terminal.

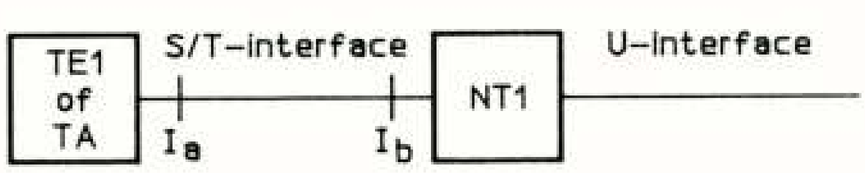
Naast de bovengenoemde voorbeelden onderscheiden we ook nog de zogenaamde faciliteiten. Deze staan niet op zich, maar vormen uitbreidingen op, of wijzigingen van drager- of telediensten. Zij ondersteunen de communicatie. Voorbeelden zijn oproep-identificatie, besloten gebruikersgroep, automatisch terugbellen bij bezet, doorschakelen, enz.

2 ISDN-toegangsstructuren

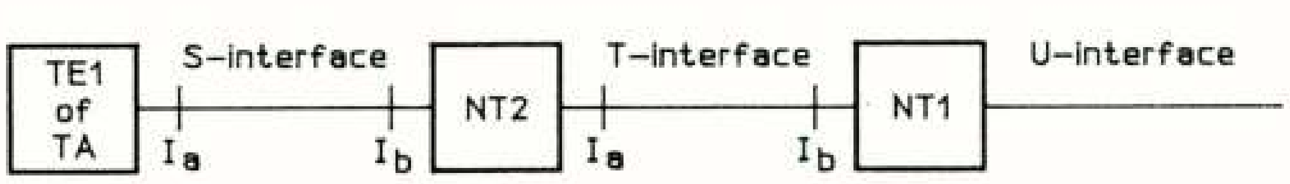
Er zijn voor de toegang tot het ISDN-net twee structuren voor het gebruikerskoppelvlak vastgelegd:

1. 'Basic Access' (2B + D)
   Deze biedt twee onafhankelijke 64 kbit/s B-kanalen voor gebruikersinformatie en een D-kanaal van 16 kbit/s voor signalering. Er zijn ook mogelijkheden om dit D-kanaal voor datacommunicatie in te zetten. De bruto-bitstroom bedraagt 192 kbit/s.
2. 'Primary Rate Access' (30 B + D)
   Het eveneens voor signalering bedoelde D-kanaal heeft hier een capaciteit van 64 kbit/s. De totale bitstroom bedraagt 2 Mbit/s.

In onderstaande figuren zijn voorbeelden van beide ISDN-referentieconfiguraties, opgebouwd uit functionele eenheden, schematisch weergegeven. De koppelvlakken hoeven niet fysiek aanwezig te zijn. Zoals aangegeven vallen bij 'Basic Access' S- en T-interface samen, bij 'Primary Rate' zullen NT1 en NT2 veelal in één apparaat geïntegreerd worden, waardoor de T-interface alleen intern aanwezig is. Tot slot moet nog opgemerkt worden dat twee kanten van de interfaces onderscheiden worden: I_a en I_b.



Figuur 1. ISDN-referentieconfiguratie voor 'Basic Access'



Figuur 2. ISDN-referentieconfiguratie voor 'Primary Rate'

Voor de overzichtelijkheid is in figuur 2 slechts één S-interface getekend. Dit kunnen er echter meer zijn.

De NT1 verricht uitsluitend transmissiefuncties, zoals lijncodering en synchronisatie. Tevens vindt er een aanpassing plaats tussen de signalen op het openbare net (dat van land tot land anders uitgevoerd kan zijn) en die op het in-huisnet (gestandaardiseerd volgens CCITT I430).
De NT2 zorgt voor de distributie van de signalen van de NT1 over verschillende S-bussen, waarop per bus maximaal acht terminals gelijktijdig aangesloten kunnen worden. Bij 'primary rate' verricht de NT2 ook schakelfuncties en is praktisch uitgevoerd als een PABX of LAN.

ISDN-terminals (TE1) worden rechtstreeks op de NT1 of NT2 aangesloten. Niet-ISDN-terminals (NT2) kunnen via een terminaladapter (TA) aangesloten worden. Als voorbeeld kan gedacht worden aan een PC met ISDN-insteekkaart. In Nederland zal, evenals elders in Europa, het T-referentievlak als scheidslijn dienen tussen de PTT-infrastructuur en het vrijgegeven terrein van de randapparatuur.

3 EMC-aspecten van ISDN

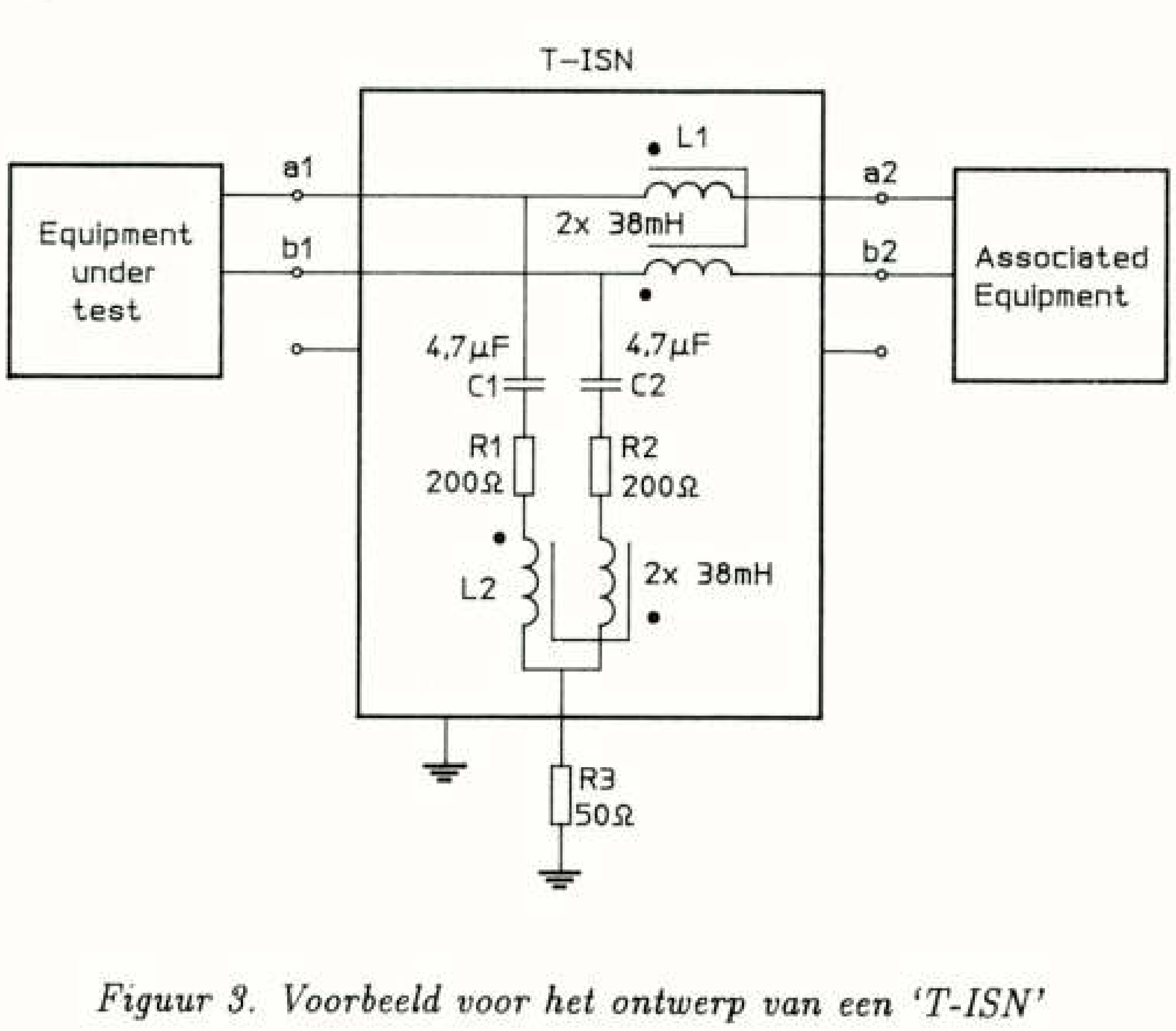
Omdat het bij de randapparatuur een geliberaliseerde markt betreft, is het noodzakelijk dat voor het betrouwbaar functioneren van een heel netwerk een zekere hoeveelheid 'basis-EMC' wordt geëist van deze apparatuur, zowel op emissie- als op immuniteitsgebied. Bij analoge systemen zijn we gewend dat als gevolg van een onvoldoende compatibiliteit een geleidelijke degradatie van de functionele eigenschappen kan optreden. Digitale systemen kunnen zich echter onder deze omstandigheden zodanig gedragen dat essentiële protocollen, nodig voor het juist functioneren van een heel netwerk, verstoord raken. Als gevolg hiervan hoeven de problemen zich niet te beperken tot één slachtoffer, maar kunnen meerdere netgebruikers de dupe zijn wanneer onvoldoende zorg is besteed is aan EMC-aspecten.

Verder is het belangrijk dat ongewenste emissie gelimiteerd wordt als bedacht wordt dat intern opgewekte klok- en transmissiesignalen frequentiecomponenten in het omroepspectrum bevatten. Bij dit laatste aspect is symmetrie een cruciaal gegeven. Overigens is dit niet alleen een zorg voor de fabrikant van de apparatuur, ook de kabelexploitant (die bij de S/T-interface niet per se de PTT hoeft te zijn) dient zijn verantwoordelijkheid te kennen.
Ook moet onderkend worden dat bij 'Primary Rate' de 2 Mbit/s T-interface (indien fysiek aanwezig en uitgevoerd met een AB-paar) uit EMC-overwegingen niet anders dan afgeschermd kan zijn.

4 EMC-normalisatie op ISDN-gebied

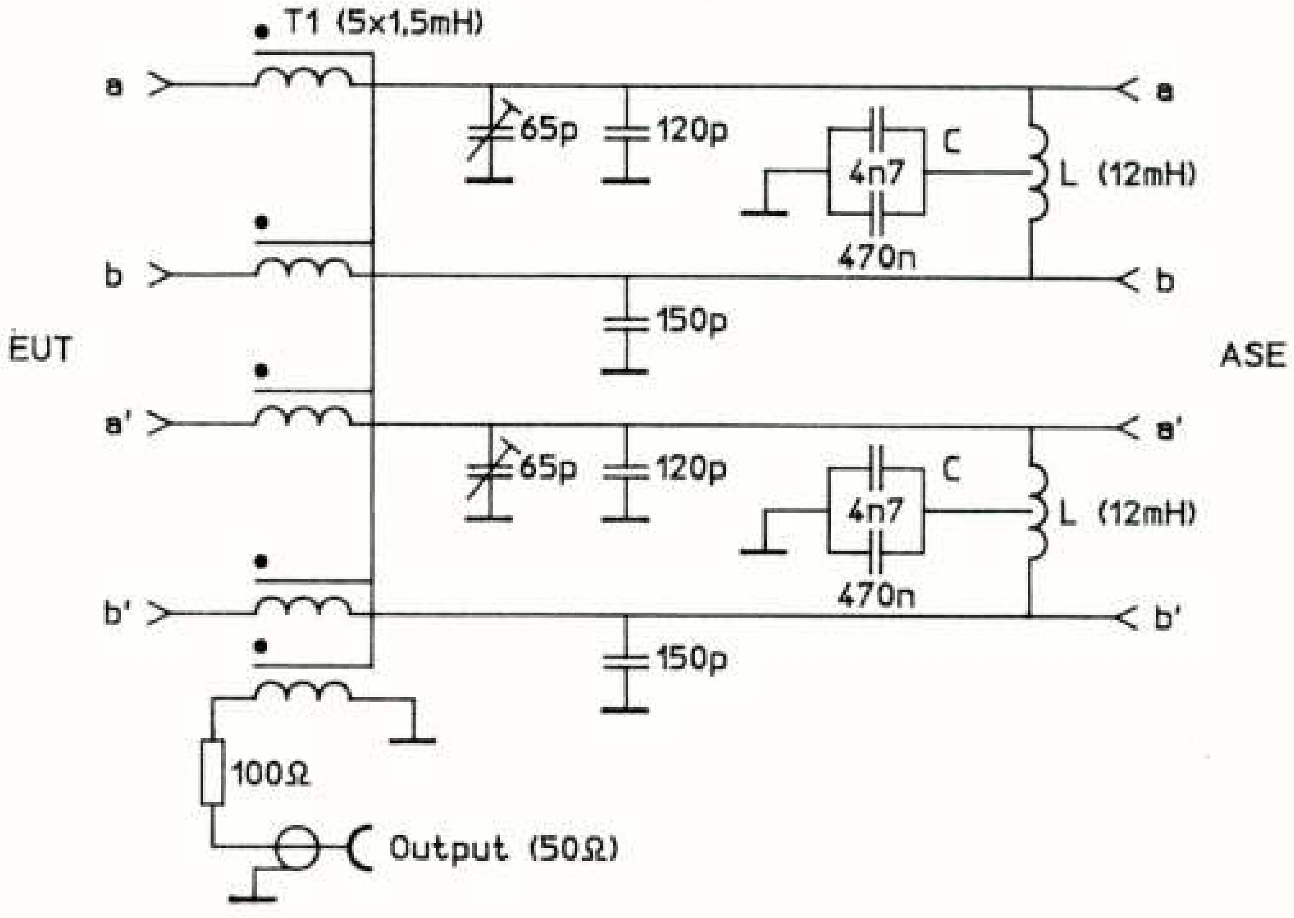
4.1 Activiteiten in CISPR G WG2

De introductie van ISDN is één van de initiatoren geweest van het normalisatiewerk dat verricht wordt op het gebied van 'conducted emission on telecommunication lines'. Deze activiteiten vinden plaats in werkgroep 2 van CISPR G en zijn erop gericht om in toekomstige edities van CISPR 22 een clausule op te nemen waarin een meetmethode gegeven wordt met bijbehorende limietwaarden voor geleidende emissie op signaalporten.
Door de grote diversiteit aan mogelijke kabels is het onmogelijk om één principe te geven voor alle mogelijke kunstnetwerken; men is het er alleen over eens dat de Common Mode impedantie 150 Ω moet bedragen.
Voorlopig wordt er onderscheid gemaakt tussen 'balanced pairs' en 'quads' enerzijds en andere kabels anderzijds. Kunstnetwerken voor de laatste categorie zijn nog 'under consideration'.
Voor telefoonlijnen bestaande uit één paar wordt de commercieel verkrijgbare 'T-ISN' voorgesteld, zie figuur 3.



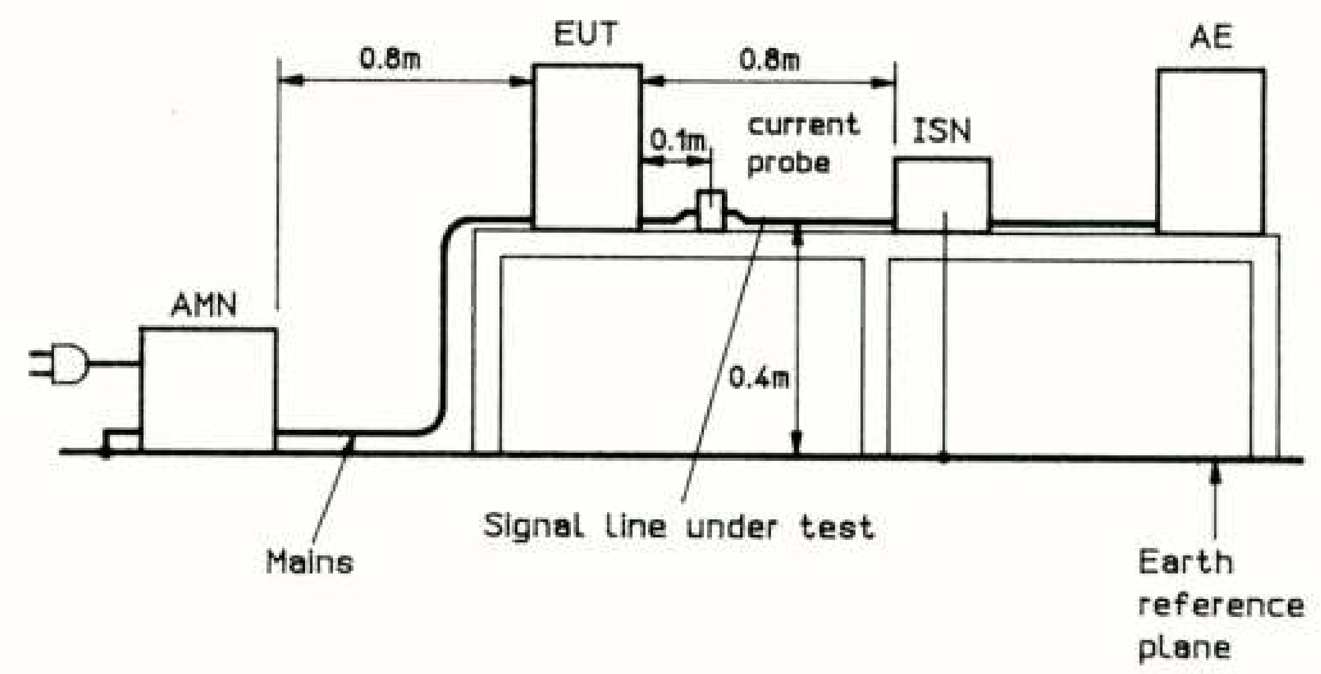
Figuur 3. Voorbeeld voor het ontwerp van een 'T-ISN'

Voor de voor ISDN belangrijke 'quads' wordt gedacht aan een combinatie van twee T-ISN's. Kritiek op dit principe heeft ertoe geleid dat er bij de laatste CISPR G WG2 vergadering voorstellen werden gelanceerd voor andere oplossingen. Het ontwerp van figuur 4 is daar een voorbeeld van.



Figuur 4. Voorbeeld voor het ontwerp van een 'quad ISN'

Voor 'table top' apparatuur is de geometrie van de meetopstelling in overeenstemming gebracht met die van de lichtnetmetingen uit CISPR 22, zie figuur 5.



Figuur 5. Meetopstelling voor 'table-top equipment'

4.2 Activiteiten in ETSI EE4

In het ETSI 'sub technical commitee' EE4 wordt de hand gelegd aan een 'product-standard' voor apparatuur met ISDN S- en T-interfaces. Door middel van 'public enquiries' wordt gewerkt aan het uitbrengen van ETS 300.126. Het emissiegedeelte verwijst naar CISPR 22 en het hierboven toegelichte amendement over 'conducted emission on signal ports', zonder hier veel nieuws aan toe te voegen.
Het immuniteitsstuk is uniek omdat op ISDN toegesneden 'compliance criteria' verbonden worden aan een aantal uit te voeren immuniteitstesten. Er is daarbij alleen teruggegrepen op de 'basic standards' uit de IEC 801 reeks of de hieraan gekoppelde TC65 secretariaatsdocumenten.

Er is getracht om uit de grote hoeveelheid niveaus, meetopstellingen en koppelnetwerken die in de IEC 801 publikaties gegeven worden, gerichte keuzen te maken die specifiek op ISDN toepasbaar zijn. In een aantal gevallen werd geen bruikbaar koppelnetwerk in de IEC 801 reeks gevonden en is er zelf een voorgesteld.

Voor een snelle indruk omtrent de immuniteitstoetsen uit Draft ETS 300.126 kan de tabel op de volgende pagina geraadpleegd worden.

Test[5]	Ref.doc.[3]	Level	Stimulus	Comp.criterium[1]	Remarks
ESD	IEC 801-2	2	4 kV	FA	Contact
			4 kV		Air
		3	6 kV	LOC	Contact
			8 kV		Air
EFT	IEC 801-4[2]	2	0,5 kV		ISDN-line
			1 kV	FA	Mains
Surges	IEC 801-5	2	1,0 kV	LOC	ISDN-line
					Mains
Cond.CW	IEC 801-6	2	3 V[4]	BER	ISDN-line
Rad.CW	IEC 801-3	2	3 V/m[4]	BER	No striplines

1)

De volgende compliance criteria zijn gedefinieerd:

BER : No bit errors
FA : No loss of frame allignment
LOC : No Loss of an ongoing communication

Anders dan bij een network termination is bij ISDN-terminal-apparatuur over het algemeen geen bit error meting mogelijk. ETS 300.126 geeft daarom voor ISDN-telefoontoestellen een criterium in termen van een akoestische geluidsdruk en voor digitale apparatuur een maximaal te tolereren percentage niet-bevestigde frames.

2)

Er is onderkend dat de burst met 'fast transients' uit IEC801-4, met name bij ISDN, een zware test vormt door de grote hoeveelheid pulsen die in korte tijd afgegeven wordt.
Bij basic access ISDN wordt informatie verstuurd in frames met een lengte van 250 μs (4 kHz). De herhalingsfrequentie van de transiënten uit een IEC 801-4 burst bedraagt nominaal 5 kHz. De toegestane afwijking van 20% sluit de mogelijkheid niet uit dat de pulsen en de frames synchroon lopen. Om deze, voor de praktijk zeer onrealistische situatie uit te sluiten, wordt nadrukkelijk gesteld dat 4,2 kHz als minimale pulsfrequentie genomen moet worden.
Bovendien mag bij het niet kunnen voldoen aan de oorspronkelijke test, de burst-herhalingsfrequentie verhoogd worden van 300 ms naar 4 s, dit om uit te sluiten dat een laag 2 protocol uit het D-kanaal continu bestookt wordt.

3)

Alleen IEC 801-2 en -4 zijn officieel uitgegeven, de rest heeft slechts een status als TC65 secretariaatsdocument en kan dus aan modificaties onderhevig zijn. In ETS 300.126 wordt daarom met nadruk gerefereerd aan gedateerde documenten.

4)

Amplitude gemoduleerd met 1 kHz, 80%.

5)

ESD: Electro Static Discharge.
EFT: Electrical Fast Transients. Een 'burst' van snelle, hoogfrequente stoorpulsen waarmee de effecten van schakelhandelingen op het lichtnet worden nagebootst.
Surges: Enkelvoudige, energierijke stoorpulsen waarmee onder andere blikseminslag wordt gesimuleerd.
Cond.CW: Conducted CW, sinusvormige amplitude-gemoduleerde signalen die met behulp van een 'kunstnetwerk' geïnjecteerd worden op de aangesloten kabels van het te testen apparaat. Frequentiegebied: 150 kHz-30 MHz.
Rad.CW: Radiated CW, sinusvormig amplitude-gemoduleerd veld waarmee het te testen apparaat wordt aangestraald. Frequentiegebied: 30 MHz-1 GHz.

4.3 Vervolg-procedure voor de ontwerp-ETS

Met de EMC-specificaties uit ETSI wordt zeker niet beoogd om meer of strengere eisen te formuleren dan in de door CENELEC geproduceerde 'generic standards' is opgenomen. Dit zou ook moeilijk te verkopen zijn aangezien CENELEC het mandaat heeft gekregen van de Europese Commissie om voor de invulling van de Europese richtlijn zorg te dragen.
De ISDN ETS moet gezien worden als een typische 'product standard'. Doordat het een goed afgebakende produktgroep betreft kan deze bovendien specifiek zijn in de beschrijving van de te hanteren testmethoden. Dit komt de vergelijkbaarheid van door verschillende onafhankelijke testinstituten verkregen meetresultaten ten goede.

Om te voorkomen dat de ISDN ETS uit de pas zou kunnen gaan lopen met de CENELEC-normen is overeengekomen dat de verwerking van commentaar uit de tweede 'public enquiry' in een werkgroep zal plaatsvinden die wordt samengesteld uit zowel ETSI- als CENELEC-leden.
Nederlands commentaar wordt verzameld via het NNI. Het 'Nederlands ETSI Leden Overleg' (NELO) is het orgaan dat deze actie coördineert.

5 Referenties

[1] CISPR G WG2 (Secretariat) 20

[2] ESTI EE4 Draft ETS 300.126 (voorheen DE/EE-4001)

Voordracht gehouden tijdens de 384e werkvergadering.

EMC-ASPECTEN VAN RADIO-ASTRONOMIE

Dr.T.A.Th.Spoelstra
Stichting ASTRON, Radiosterrenwacht Dwingeloo

Allerlei door de mens veroorzaakte storing heeft in toenemende mate een negatieve invloed op sterrenkundige waarnemingen. Veel, zo niet alle, radiosterrenwachten ervaren op de een of andere manier degradatie van de waarnemingen. Een strategie om activiteiten op mondiaal niveau te coördineren met het doel deze storing te bestrijden moet verbeterd worden, terwijl overleg met actieve gebruikers van het spectrum en de verantwoordelijke overheidsinstanties uitgebreid moeten worden. Vooral met het oog op de algemene World Adminstrative Radio Conference, die onder auspiciën van de Internationale Telecommunicatie Unie in 1992 gehouden wordt, is dit uiterst dringend. Op deze conferentie worden alle toewijzingen van frequenties tussen 0.5 en 3 GHz geheel opnieuw bezien, tezamen met die voor 'nieuwe diensten' op frequenties boven 20 GHz.

1. INLEIDING

Steeds meer hebben radiosterrenkundige waarnemingen te lijden van allerlei storingen in de buurt van of zelfs in de aan radioastronomie toegewezen frequentie banden. Met nieuwe technologieën, zoals zenders in de ruimte en het gebruik van "spread-spectrum" technieken, vreet het storings-probleem binnen de radiosterrenkunde steeds verder om zich heen. Anderzijds neemt de kwetsbaarheid voor storing steeds meer toe, omdat binnen de radiosterrenkunde steeds gewerkt wordt aan betere gevoeligheid en grotere ontvanger-bandbreedten. Het probleem is het conflict tussen passief en actief frequentie-gebruik.

Radiofrequenties worden toegewezen aan de verschillende gebruikers/toepassings-groepen ofwel "diensten" op World Adminstrative Radio Conferences (WARCs), die onder auspiciën van de Internationale Telecommunicatie Unie (ITU) gehouden worden. De leden van de ITU zijn soevereine landen, die op WARCs vertegenwoordigd worden namens nationale overheden. Deze overheidsvertegenwoordigers kunnen bijgestaan worden door derden, die als waarnemer op WARCs aanwezig kunnen zijn. Voor radiosterrenkunde is dit de Inter Union Commission on the Allocation of Frequencies (IUCAF). IUCAF is ingesteld door de International Council of Scientific Unions (ICSU) en haar leden hebben zitting namens de Internationale Unie van Radiowetenschappen (URSI), de Internationale Astronomische Unie (IAU), en de Internationale Commissie voor Ruimte Onderzoek (COSPAR).

Radiofrequenties kunnen worden toegewezen met een primaire, secundaire of een voetnoot status. De situatie is nog ingewikkelder, daar de toewijzingen afhankelijk zijn van het gebied op aarde. De frequentie toewijzingen worden bijgehouden in de Radio Regulations (RR) van de ITU. In de RR is radiosterrenkunde een van de vele diensten.

2. ACTIEF EN PASSIEF

In de radiosterrenkunde wordt geen signaal door de mens uitgezonden en daarom is hier sprake van een passief frequentie gebruik. Radiosterrenkunde heet dan ook een passieve dienst. Het doel van elke dienst is om aan de ontvangerkant een zo goed mogelijke signaal-ruis-verhouding te bereiken. In het algemeen wordt het zendervermogen aangepast om een goede ontvangst te bewerkstelligen.

Voor sterrenkundig onderzoek is de beschikbaarheid van het gehele electromagnetisch spectrum van essentiëel belang: verschillende fysische processen veroorzaken electromagetische straling bij verschillende frequenties. Voor elk frequentie-domein zijn instrumenten beschikbaar.

Radiosterrenkunde kan dus geen enkele invloed uitoefenen op het uitgezonden signaal. Het uitgezonden vermogen kan niet aangepast worden om de detecteerbaarheid te verbeteren. De frequenties van spectraallijnen, die voor radioastronomisch onderzoek belangrijk zijn, kunnen niet door de mens verschoven worden, omdat ze gedicteerd worden door de natuurkundige omstandigheden in de radiobron en door het medium, waar het signaal doorheen trekt. Ook aan de ontvangerkant zijn dus geen vrijheden voor de frequentiekeuze. Schema 1 geeft deze mogelijkheden samenvattend weer.

Radiosterrenkunde ontvangt kosmische ruis. Het is dus intrinsiek een analoge dienst. De signalen zijn uiterst zwak: een detectie van typisch 60 dB onder ontvangerruis is tegenwoordig geen probleem. Dit staat in scherp contrast met een 20 dB boven ontvangerruis, wat karakteristiek is voor actief frequentie gebruik. Daarbij komt ook, dat in dit laatste geval de mens aan de zender- en ontvangerkant alle gewenste aanpassingen kan maken om een zo goed mogelijke signaal-ruis-verhouding te bereiken. Samenvattend is dit weergegeven in

schema 2.

3. EMC RELATIES

Radio astronomen ontvangen slechts radiostraling. Deze straling is van buitenaardse oorsprong, en daardoor zijn alle stralingseigenschappen door de natuur gedicteerd. Sterrenkundigen hebben daarom alleen maar de electromagnetische omgeving van de ontvanger in de hand en dit schept een conflict met actieve gebruikers van het radiospectrum. En aangezien het electromagnetisch spectrum een eindige verdeling toelaat en een "passieve" dienst dezelfde frequenties niet echt met een "actieve" dienst kan delen, vallen frequentie toewijzingen aan passief gebruik onder de uiterst schaarse "natuurlijke rijkdommen".

	zender/bron aanpassen	**ontvanger aanpassen**
vermogen/ gevoeligheid aanpassen	**neen**	**ja**
frequentie aanpassen	**neen**	**neen**

Schema 1: keuze-vrijheid van de mens: radiosterrenkunde

	zender/bron aanpassen	**ontvanger aanpassen**
vermogen/ gevoeligheid aanpassen	**ja**	**ja**
frequentie aanpassen	**ja**	**ja**

Schema 2: keuze-vrijheid van de mens: actief frequentie gebruik

Het is duidelijk, dat hiermee ook de omvang van het EMC probleem gegeven is, waarmee radiosterrenkunde zich geconfronteerd ziet. We kunnen de EMC relaties samenvattend volgens schema 3, terwijl de problematiek gegeven samengevat wordt in schema 4. We onderscheiden de volgende relaties:

-1- tussen een niet-zender en een niet-ontvanger. De EMC problematiek betreft de onderlinge electromagnetische wisselwerkingen tussen bijvoorbeeld huishoudelijke apparatuur (zoals magnetrons) en computerapparatuur.

-2- tussen een niet-zender en een ontvanger. Dit is typisch de plaats, waar we passief frequentiegebruik vinden. Het EMC probleem betreft bijvoorbeeld gangbare problemen, waarvoor radiosterrenkunde geplaatst is: niet voor niets zijn storingvrije zones rond de radiosterrenwachten van Dwingeloo en Westerbork aangebracht: om electromagnetische storingen van bijvoorbeeld verkeer te weren.

-3- tussen een zender en een niet-ontvanger. Of anders gezegd: het functioneren van electronische apparaten in sterke velden (bijvoorbeeld in de buurt van een zender). Het betreft hier relaties van deze zender tot apparatuur, die door alle frequentiegebruikers benut wordt.

-4- tussen een zender en een ontvanger: in actief spectrum gebruik beoogt men deze relatie zo goed mogelijk te maken. In passief spectrum gebruik wil men juist slechts radiostraling ontvangen van die bron, waarin men interesse heeft en kan men storing van andere oorsprong niet verdragen. Een goede EMC benadering vereist voor deze relatie dan ook deugdelijke afspraken. En het zijn die afspraken, die met locale overheden (= binnen een beperkt gebied, binnen een land), regionale overheden (= in een gebied van meerdere landen, bijvoorbeeld Europa) en in mondiaal verband (= op wereldschaal: daarvoor staat de ITU) steeds getoetst moeten worden op hun relevantie. Waar nodig moeten ze aangepast worden, aangescherpt of vervallen verklaard worden.

De kwetsbaarheid van een passieve dienst verschilt wezenlijk van andere radio diensten, waarvoor het nodig is zowel te zenden als te ontvangen (om deze reden worden deze actieve diensten genoemd). Daar een passieve dienst nimmer storing kan veroorzaken aan een actieve dienst, zijn de problemen voor een passieve dienst altijd het gevolg van actief gebruik van frequentiebanden, die aan passieve toepassingen toegewezen zijn.

De oorsprong van het probleem voor radiosterrenkunde is, dat bij de eerste toewijzing van radiofrequenties aan de dienst Radio Astronomie (op de WARC in 1959) men deze had moeten onderkennen als een passieve dienst, die veel kwetsbaarder dan andere diensten vanwege de veel hogere gevoeligheid voor storing. Een herdefinitie is echter ondenkbaar. Toch zou deze wenselijk zijn, daar in de RR een "passieve dienst" als zodanig niet gedefiniëerd is. Vanwege deze vaagheid is het van belang adequate richtlijnen voor de overheidsadministraties te hebben, omdat frequentiebanden in gebruik kunnen zijn door "passieve" diensten, hoewel in die banden geen communicatie met behulp van monitoring waargenomen kan worden. Adequate richtlijnen zijn voor de overheden steeds meer van belang vanwege de toenemende druk voor actief gebruik van radio frequentie banden geleid door commerciële motieven.

	niet-ontvanger	ontvanger
niet-zender	*1.* **electromagnetische wisselwerking tussen electronische apparatuur**	*2.* **passief spectrum gebruik (radiosterrenkunde)**
zender	*3.* **actief, passief spectrumgebruik en electronische apparatuur**	*4.* **actieve + passief spectrum gebruik**

Schema 3: EMC relaties

		gevolg	
		niet-ontvanger	ontvanger
oorzaak	niet-zender	*1.* **het algemene probleem van het kunnen samenleven van electronische apparaten**	*2.* **de "bestaansreden" van de storingsvrije zones bij Dwingeloo en Westerbork**
	zender	*3.* **het functioneren van electronische apparaten in sterke velden (bijv. dicht bij een zender)**	*4.* **"afspraken" over spectrumgebruik**

Schema 4: EMC probleemvelden

4. PROBLEEMRUIMTE

De storingsproblemen in de radiosterrenkunde kunnen onderscheiden worden in verschillende categorieën afhankelijk van hun afstand tot de storingsbron. We kunnen onderscheid maken tussen mondiale, regionale en locale probleem (zie figuur 1).

Mondiale problemen worden voornamelijk veroorzaakt door satellietsystemen. Satellietsystemen, die momenteel de radiosterrenkunde het sterkst storen zijn:

[i] Global Positioning System, GPS: de USA zijn reeds een aantal jaren bezig met het opzetten van een Global Positioning System, GPS, dat uiteindelijk uit 18 satellieten moet bestaan en dat gebruikt wordt voor plaatsbepaling op aarde. Doel is om op elk moment tenminste 4 satellieten boven de horizon 'zichtbaar' te hebben. Een van de banden, die GPS gebruikt is de L3-band, van 1360-1440 MHz, die een directe bedreiging is voor de radioastronomische 1400-1427 MHz band. Vanwege vervelende neveneffecten zijn filters in GPS ingebouwd. Aangezien de WARC 1979 besloot, dat "no intended emission" toegestaan is in de 21 cm band, overtreedt GPS de RR. Recente waarnemingen, die op verschillende sterrenwachten rond 18 cm golflengte gedaan werden, hadden te lijden van ernstige storing. Monitoring metingen op het Onsala Space Observatory wezen onomstotelijk zijlus effecten van GPS satellieten als oorzaak aan. Het storingsniveau liep op tot 13 dB boven de aanbevelingen van de CCIR (Spoelstra en Kahlmann, 1990a).

[ii] GLONASS: De Sovjet Unie ontwikkelt een satellietsysteem, waarvan GPS feitelijk afgekeken is, GLONASS. GLONASS opereert rechtmatig binnen de toegewezen frequentiebanden. Echter, ernstige problemen met zijlussen veroorzaken forse storing met gebruik door passieve diensten zoals radiosterrenkunde van banden rond 18 cm golflengte (voor radiosterrenkunde en belangrijk frequentiegebied, omdat daar straling van het OH-radicaal uitgezonden wordt). Hoewel de primaire emissie van het systeem in de toegewezen banden geschiedt, voldoen de zijlussen niet aan de CCIR specificaties. Momenteel moet meer dan 50-70% van radiosterrenkundige waarnemingen bij 18 cm golflengte als verloren beschouwd worden door GLONASS. Echter, radiosterrenkunde heeft slechts een secundaire allocatie in de betreffende banden (Spoelstra en Kahlmann, 1990b).

[iii] mobile-satellite service: een belangrijke bron van storing is vliegtuig-satelliet communicatie en satelliet-satelliet communicatie. De 1-2 GHz band is het meest geschikt voor mobiele satelliet systemen. De 0.8-0.9 GHz band wordt niet gebruikt in Europa. De 1.5-1.6 GHz band is bestemd voor de mobile-satellite-service (MSS). Deze toepassing lijkt een grote bedreiging voor radiosterrenkunde te worden.

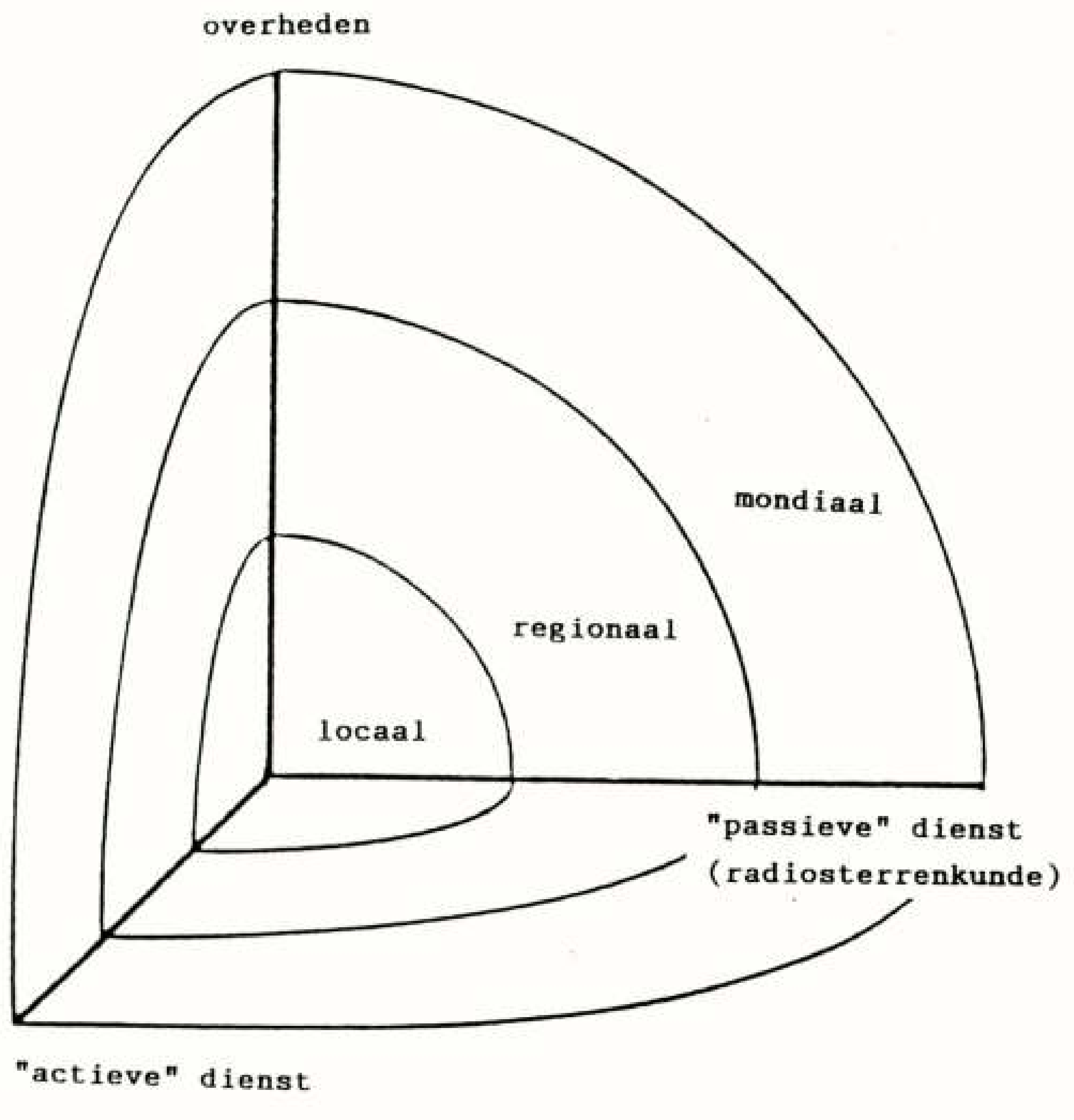


Fig. 1: "Probleemruimte" EMC problematiek radiosterrenkunde

Regionale problemen worden voornamelijk veroorzaakt door TV in frequentiebanden net naast door radiosterrenkunde gebruikte banden of zelfs binnen deze banden. Deze problemen zijn in Europa, het Amerikaanse continent, Azië, Afrika en Australie telkens verschillend. In Europa is een zeer groot probleem de TV in de 608-614 MHz band (kanaal 38). In sommige landen is deze band momenteel vrij voor radiosterrenkunde, terwijl in andere landen TV zenders op deze frequenties in gebruik zijn. In de ITU RR wordt er overigens bij de overheden op aangedrongen om zoveel mogelijk radiosterrenkunde te ontzien.

Locale problemen: in beginsel treden locale problemen alleen maar op in de buurt van de radiosterrenwacht. Ze moeten dan ook locaal opgelost worden. In Europa is TV in kanaal 38 een groot probleem in Italië (waar sedert eind 1989 op frequenties beneden 1.4 GHz geen waarnemingen meer mogelijk zijn) en Polen. Bovendien is in Italië een grote moeilijkheid, dat een deugdelijke overheidsorganisatie en rechtspraak in frequentiezaken ontbreken.

Andere problemen zijn in sommige landen vliegtuig-radar.

In beginsel zijn locaal oplossingen te vinden voor al deze toepassingen van het spectrum. Dit ligt geheel anders met storingen, die afkomstig zijn van niet geregistreerde apparatuur, zoals huishoudelijke apparaten (magnetrons, draadloze telefoons, e.d.) en garagedeuropeners.

Door de toenemende druk op radiofrequenties ziet de toekomst er voor radiosterrenkunde zorgelijk uit. Grote mondiale en regionale ontwikkelingen, die in potentie elk binnen hun frequentiegebied "dodelijk" zijn voor radiosterrenkunde, zijn samengevat in Tabel 1.

Daarnaast zijn als een nieuwe ontwikkeling voorstellen tot commercialisatie van frequentie management te verwachten. De argumentatie hiervoor is, dat de deregulering en privatisering van telecommunicatie en omroep in een aantal landen geleid heeft tot een toegenomen druk op toegang tot gebruik van radio frequenties. Dit bracht enkele regeringen, te weten Verenigde Staten, Australië en Nieuw Zeeland, ertoe om de verantwoordelijkheden voor de toewijzing van radiofrequenties opnieuw te bezien en de toewijzing te laten beheersen door een marktmechanisme en niet meer door bureaucratie. De idee is, dat vanwege het feit, dat het radiospectrum zo'n kostbaar goed is, het van vitaal belang is, dat slechts die gebruikers, die dit goed op zijn juiste waarde weten te schatten, daar toegang toe hebben. En ook is de idee, dat "eigendomsrechten" in het spectrum gecreëerd kunnen worden, die weer kunnen worden gekocht en verkocht, verzameld en verdeeld zoals land of andere grondstoffen. In de praktijk betekent dit niet alleen, dat men moet betalen voor (bepaalde) frequenties, maar ook, dat men een boete krijgt, wanneer die frequentie band niet juist gebruikt wordt (: hoe is dit te realiseren voor een passieve dienst als radiosterrenkunde? ...).

De mondiale problemen worden ook steeds belangrijker vanwege het toenemende gebruik van Very Long Baseline Interferometry (VLBI) toepassingen. Met deze techniek worden waarnemingen gedaan met radiotelescopen, die op onderlinge afstanden van vele duizenden kilometers van elkaar verwijderd staan en waarvan de gegevens op magneetbanden van zeer hoge dichtheid opgeslagen worden om vervolgens in een centrale verwerkingseenheid gezamenlijk afgespeeld te worden, met het oog op correlatie van de waargenomen signalen. Deze techniek wordt routinematig al meer dan 20 jaar toegepast en heeft bewezen zeer waardevol te zijn voor het onderzoek van structuren met zeer kleine hoekafmetingen. Het is geen probleem meer om resoluties voor hoekafmetingen van 0".0003 te behalen met intercontinentale VLBI. Veel landen nemen actief deel aan het VLBI onderzoek.

VLBI is dan en alleen dan mogelijk, wanneer de gebruikte frequentiebanden wereldwijd dezelfde be-

Tabel 1

Ontwikkelingen met onmiddellijke dreiging voor radiosterrenkunde

Frequenties (GHz)	toepassing	reikwijdte
0.608 - 0.614	TV	locaal/regionaal
1.427 - 1.530	Broadcasting-Satellite Service	regionaal
1.610 - 1.6265	Radio Determination Satellite System	regionaal
1.645 - 1.660	two-way satellite band	regionaal/mondiaal
1.6565- 1.6605	Land Mobile Satellite Service	regionaal/mondiaal
1.660 - 1.6605	Public Correspondence	mondiaal
21.2 -23.6	High Definition Television, HDTV	regionaal/mondiaal

scherming genieten. Dit geldt met name voor frequenties rond 0.3, 0.6, 1.4, 1.6, 5.0 en 22 GHz.

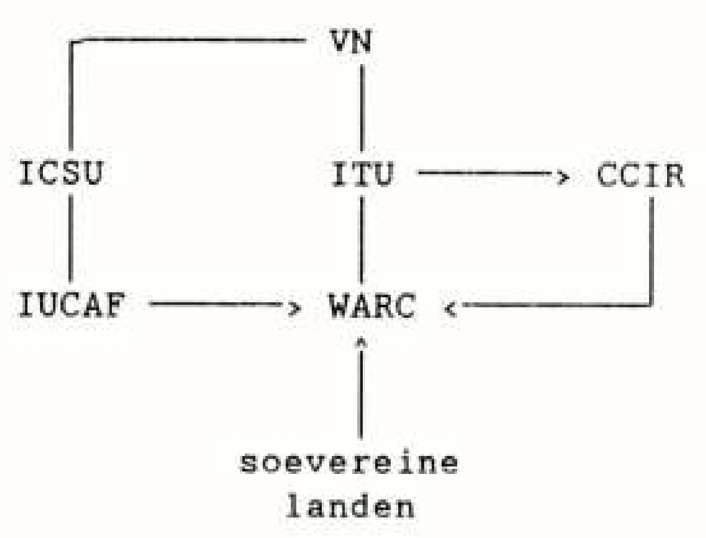
De techniek van VLBI heeft veel andere praktische toepassingen, zoals het onderzoek naar het tempo van de aardrotatie, continentale drift, poolbeweging, bepaling van geografische breedte en voorspelling van aardbevingen. Dergelijke experimenten stellen ons in staat intercontinentale afstanden te meten met nauwkeurigheden van enkele centimeters.

5. ITU, CCIR, WARC

Zoals gezegd worden radiofrequenties toegewezen aan de verschillende gebruikers/toepassings-groepen ofwel "diensten" op World Adminstrative Radio Conferences (WARCs), die onder auspiciën van de Internationale Telecommunicatie Unie (ITU) gehouden worden. De leden van de ITU zijn soevereine landen, die op WARCs vertegenwoordigd worden namens nationale overheden en elk één stem hebben. Deze overheidsvertegenwoordigers kunnen bijgestaan worden door derden, die als waarnemer op WARCs aanwezig kunnen zijn, zoals IUCAF. De technische commissie van de ITU, de International Radio Consultative Commission (CCIR) bereidt technische adviezen en richtlijnen voor ten behoeve van verantwoord frequentiebeheer en WARCs. Samenvattend is de organisatie rond een WARC gegeven in schema 5.

Om tot deugdelijke technische adviezen en richtlijnen te komen, worden de werkzaamheden binnen de CCIR in verschillende studiegroepen uitgevoerd.

Ten aanzien van de technische aspecten van frequentiemanagement voor radiosterrenkunde heeft IUCAF de taak om voorstellen en adviezen te ontwikkelen en onderzoek te initiëren. IUCAF kan technische voorstellen en adviezen bovendien bespreken met nationale en internationale organisaties. Aangezien het karakter van IUCAF mondiaal is, is het niet altijd mogelijk dat zij zich regionaal adequaat van haar taak kan kwijten. Om hierin te voorzien werkt als ondersteuning van IUCAF onder auspiciën van de European Science Foundation (ESF) te Straatsburg de Commissie voor Radio Astronomische Frequenties (CRAF). CRAF heeft als taak op regionaal Europees niveau te werken aan storingsbestrijding binnen radioastronomische frequentiebanden. CRAF staat tevens in een overleg relatie met de Conference Européenne des Postes et des Telecommunications (CEPT). Binnen de Verenigde Staten werkt met dezelfde doelstelling het Commitee voor Radio Frequenties (CORF). CORF is een commissie van de Amerikaanse National Science Foundation (NSF). CORF en CRAF functioneren beide als een studiegroep ten behoeve van IUCAF. Daarnaast initiëert en verricht CRAF technisch onderzoek naar technieken voor storingsonderdrukking.



Schema 5: Organisatie structuur WARC

Het grote belang van een goede verdeling van radiofrequenties over alle diensten met het doel om deze ongestoord te kunnen gebruiken staat buiten kijf. Daarnaast zijn er nog een paar gegevens:

- niet in alle landen vinden alle diensten een toepassing. Frequentiegebruik ten behoeve van bijvoorbeeld ruimtevaart, radiosterrenkunde, (ontwikkeling van) radioplaatsbepalingssystemen, satelliet-omroep en moderne hoogwaardige technologie vindt men lang niet in alle landen.
- de commerciële druk bij ontwikkeling van geavanceerde satelliet-toepassingen neemt enorm toe vanwege de financiële belangen, die grotere omvang hebben dan

astronomische bedragen.

- verschillende landen beoordelen ter tafel liggende voorstellen verschillend om uiteenlopende redenen.

Vanwege deze aspecten is het noodzakelijk voor elk van de diensten overleg te bundelen en zoveel mogelijk steun voor haar aanvragen/voorstellen te verkrijgen. Aangezien ze niet zelf aan het overleg kunnen deelnemen en nog minder stemrecht hebben, moeten ze door lobbymethoden trachten zoveel politieke steun voor hun standpunt te verkrijgen.

Omdat bovendien elk land slechts één stem heeft en het toch voor zich het maximale profijt uit de conferentie wil halen, zullen de landen onderling overleggen of tot blokvorming komen om het beoogde doel te bereiken.

Deze verpolitisering blijkt steeds verder om zich heen te grijpen. Een technische commissie als de CCIR blijkt ook allang niet meer van politieke smetten en infecties vrij te zijn. Een gevolg van deze ontwikkeling is, dat technisch overleg minder aandacht krijgt dan wenselijk zou zijn en politieke lobbies het toneel gaan overheersen ten koste van de deugdelijkheid van de technische regelgeving en adviezen voor verantwoord spectrumgebruik. Hierdoor wordt de EMC problematiek ook steeds meer een probleem, dat met politieke (en aan de aard van het probleem vreemde) middelen benaderd moet worden.

Voor radiosterrenkunde staat op de WARC in 1992 zeer veel op het spel: het voortbestaan van deze wetenschap in de frequentiebanden 0.5 - 3 GHz en boven 20 GHz. Via de geëigende kanalen tracht zij voor het onderzoek noodzakelijke frequenties te behouden. Echter, zij heeft geen geld en geen politieke invloed, terwijl wereldwijd grote investeringen ten behoeve van dit onderzoek gedaan zijn. Over het geheel genomen gebruikt radiosterrenkunde overigens nauwelijks 1% van het beschikbare radiospectrum. Dit geeft aan, dat indien alle radioastronomische frequenties aan andere diensten toegewezen worden, de problemen, die aanleiding voor deze (vervroegde) WARC zijn en welke daar verder ter tafel komen, niet opgelost worden, maar wel enorme kapitaalvernietiging bij radiosterrenkunde tot gevolg hebben.

6. LITERATUUR

Spoelstra, T.A.Th., Kahlmann, H.C., 1990a, "Interference Problems in Radio Astronomy - VI", Netherlands Foundation for Research in Astronomy, Internal Technical Report 194.

Spoelstra, T.A.Th., Kahlmann, H.C., 1990b, "Interference Problems in Radio Astronomy - VIII", ESF-CRAF-M-08.

Voordracht gehouden tijdens de 384e werkvergadering.

THE REQUIREMENTS FOR EUROPEAN STANDARDS ON ELECTRO MAGNETIC COMPATIBILITY

Ir. M.C. Vrolijk

Philips Concern Standardization Department, Eindhoven

1. Aim

The aim of this article (based on a lecture held for NERC on 12 December 1990) is to increase the awareness that new EMC standards are necessary to enable manufacturers to place apparatus on the community market, without mandatory typetesting by a third party.

A review will be given which standards are already available and how Cenelec intends to solve the problem for consumer goods and information technology equipment on short notice and for other professional products at a somewhat longer timescale.

2. Problem area

The European Council Directive relating to Electro Magnetic Compatibility (89/336/EEC), which covers in fact all electrical and electronic equipment and systems, contains one article which create particularly the problem. Article 10.2 requires a manufacturer or importer to hold at the disposal of the authorities a technical report or certificate (issued by a third party testing institute), concerning each type of apparatus for which no standards exist on emission and immunity or for which the manufacturer has deliberately deviated from existing standards in his design. Moreover a technical file must be made concerning the technical product documentation and the measures taken to ensure conformity with the objectives of the Directive. These are described as adequate levels of emission and immunity which allow other apparatus and the apparatus itself to operate as intended.

To incline manufacturers to participate in standardization work, article 10.1 describes the procedures in case that standards exist and the manufacturer has applied these standards in his product. In that case the product may be placed on the market without any mandatory type testing. Only a manufacturer's declaration that the product is in conformity with the standards must be held available. As nothing is mentioned in this article 10.1 about technical product documentation or test results, I take it for granted that in case of dispute the proof of evidence is at the side of the relevant competent authorities.

The following problems exist:

- there are only a limited number of European emission standards and only one European immunity standard.
- the capacity of the existing testing institutes is insufficient to deal with all required tests after 1991, when the Directive comes into force.
- in the absence of standards the criteria for approval fail which will lead to unequal treatment by different test houses.
- innovative products, for which in general the standards are being made after some years of experience, will probably get their try-out outside the community market because of the barrier of type testing and the time-delay involved.
- the equal application of the Directive in the twelve Member States is probably the most severe problem. National authorities have the obligation to inspect the market. But how stringent will that be carried out? As an example: the testing of a washing machine on emission and immunity takes about three weeks by skilled experts in a well-equipped laboratory. A minimum number of three models must be tested to gather statistical information before a dispute can be started (for click measurements even seven models are required).

  Moreover the National Authorities shall inform the European Commission of any measure, like withdrawing an apparatus from the market or restricting its free movement, indicating the reasons. Therefore National Authorities will not easily withdraw an apparatus from the market.

3. Product areas

The Directive covers all apparatus which may cause electromagnetic disturbance or which may be susceptible to electromagnetic disturbance.

Apparatus means here all electrical and electronic appliances together with equipment and installations containing electrical and/or electronic components. It is likely that "components" themselves (e.g. IC's, μP's etc.) are excluded by this definition, although they themselves are in general containing electronic components.

On the other hand installations are included, which may cover high-voltage power networks for train and tramway, public telecommunication networks and local area networks. But also trains, airplanes, ships, trams and trolleybuses are included (ignition systems of motor vehicles are exempted).

In the Directive a non-exhaustive list is given in Annex III of apparatus covered by the Directive. It is

obvious that the following apparatus are also included: industrial, medical, scientific equipment, consumer electronics, domestic appliances, lighting devices and information technology equipment, telecom equipment, alarmsystems and office equipment, as well as military equipment.

Also special apparatus are covered, such as apparatus inboard ships and aeroplanes, in switching stations for offshore application. In fact all mains coupled equipment and battery powered devices are included.

4. Available standards

Untill the introduction of the "new approach" Directives which have an umbrella function, covering a variety of equipment, the European standardization institute Cenelec was mainly focussed on the formulation of dedicated product standards and family standards.

Since 1984, when the technical Committee Cenelec CISPR was revived the following emission standards were adopted, dealing with the radio frequency spectrum and all based on work prepared by IEC CISPR:

- EN 55014 Household appliances and portable tools
- EN 55015 Luminaires and fluorescent lamps
- EN 55022 Information technology equipment
- EN 55011 Industrial scientific and medical equipment
- EN 55013 Radio broadcast receivers

and one immunity standard

- EN 55020 Radio broadcast receivers.

For the emission of lower frequency signals to the mains by household equipment connected to the mains, Cenelec has adopted the European standard EN 60555 concerning "Household appliances", based on work carried out by IEC TC77.

For the immunity of industrial process measurement and control equipment a series of standards were developed by IEC TC 65. These standards concern immunity to electrostatic discharge, radiated e.m. fields, transients, surges and injected currents. Some of these standards are already adopted as harmonized document HD 481.

However the progress of about one EMC standard per year is too slow to fulfil the urgent need for standards for all equipment, apparatus and systems covered by the EMC Directive, before the end of 1991 when this Directive comes into force.

5. Solution by CENELEC

A new approach for EMC standards was adopted by Cenelec, end 1988. To this purpose a new Technical Committee, TC 110 was established, which is responsible for the whole range of standards necessary for the E.M.C. Directive. The committee Cenelec-CISPR was transformed into Sub-committee 110A, responsible for emission and immunity standards for Information Technology Equipment (including Telecom Terminal Equipment) and the harmonization in Cenelec of IEC-CISPR Publications.

Instead of formulating a big number of dedicated product standards, only a few generic specifications should be made containing the minimum requirements for all equipment and systems to enter the market.

To make these requirements as realistic as possible the phenomena which occur in several application areas should be studied and a classification of the environment should be made, especially for immunity requirements.

This is good in theory but difficult to carry out in practice.

First of all there are too many phenomena and most of the phenomena are varying in time and place. They are also dependent on the equipment placed in that environment. The value to be measured is also influenced by the measuring method, which need to be standardized first. After that, it will take years of hard labour by a big number of skilled experts to gather the figures for a statistical evaluation of the several environments.

A more pragmatic approach for which was chosen is the division of the environment in three application areas:

1. domestic, office and light industry
2. heavy industry
3. special areas.

For certification purposes and type testing it is not sufficient to have an excellent classification of the environment.

Classes for equipment need to be derived which can be tested in the laboratory in a reproduceable way, for each selected phenomenon separately. The tests must be cheap and easily to perform.

For each application area a generic emission and a generic immunity standard need to be formulated, leading to three classes of equipment.

The manufacturer needs to indicate in his manufacturer's declaration to which standard his equipment conforms to. He may also indicate the application area in his instructions for use. However, according to article 3 of the Directive the responsibility for correct application remains at the users side.

The highest priority has been given to formulate requirements for the first class, for a limited number of the most obvious phenomena and to base the limit values mainly on the experience of the manufacturers with existing equipment combined with theoretical considerations.

The following generic standards are prepared and brought under vote, with closing date October 1991:

- pr.EN 50 081-1 Generic Emission Standard. Part 1:

Domestic, Commercial and Light Industry

- pr.En 50 082-1 Generic Immunity Standard. Part 1: Domestic, Commercial and Light Industry.

When adopted, generic standards are applicable to products for which no specific product standard on emission or immunity exists. The existing or later developed specific product standard takes precedence over generic standards.

For industrial equipment, generic standards are in preparation.

Two immunity standards for Information Technology Equipment will be brought into the parallel voting procedure in IEC and Cenelec, Spring 1991. It concerns:

- pr.EN 55 101-2 Electrostatic discharges on I.T.E.
- pr.EN 55 101-3 Radiated fields on I.T.E.

It may be concluded that for the majority of equipment no immunity problems exist in practice and that by consequence all testing, certification, E-marking and the administration of manufacturer's declaration ad to the cost of products to no benefit of the user. However, the user has to pay for it.

Voordracht gehouden tijdens de 384e werkvergadering.

DE IMPLEMENTATIE VAN DE EMC RICHTLIJN

Ing. C.L. Nijdam
Ministerie van Verkeer en Waterstaat
Hoofddirectie Telecommunicatie en Post (HDTP)

The implementation of the EMC directive. This article summarises the main provisions of the Electromagnitic Compatibility Directive, the fourth of the so called "new approach" directives. In contradiction to the old directives new approach directives do not contain detailed technical requirements but in general terms described "essential requirements". Applying European Standards will be the main way for manufacturers to demonstrate that these requirements have been satisfied. The directive will be implemented in the law by 1 July 1991 and will come into force by 1 January 1992. The directive has a transitional period of 1 year, which, at the moment of writing this article (December 1990) is still subject of discussion between the Commission and the Member-states. This directive will affect large sections of the manufacturing industry as well as the wholesalers and importers.

Inleiding

De Europese regelgeving op het gebied van EMC (Elektromagnetische compatibiliteit) bestond tot nu toe uit een drietal richtlijnen. Deze richtlijnen bevatten limietwaarden en meetmethoden voor de elektromagnetische emissie van verbrandingsmotoren van automobielen, huishoudelijke apparaten/draagbaar gereedschap en fluorescentie verlichting. Aanpassing van deze richtlijnen aan nieuwe ontwikkelingen is nogal omslachtig, omdat daarvoor het volledige regelgevende proces van de EEG moet worden doorlopen. De richtlijnen bestrijken slechts enkele produktgroepen en stellen uitsluitend eisen aan emissie en niet aan immuniteit.

Pogingen om de Europese regelgeving uit te breiden naar andere produktgroepen en fenomenen zijn in het verleden altijd vastgelopen. Een aantal Lid-staten stelt daarom in aanvulling op de Europese regelgeving emissie- en zelfs immuniteitseisen aan bijvoorbeeld informatieverwerkende apparatuur, omroepontvangers enz. Hoewel op zich vaak begrijpelijk leidt eigen regelgeving van Lidstaten tot handelsbarrières.

Op 7 mei 1985 besloot de Raad van Ministers tot een "Nieuwe Aanpak" voor technische harmonisatie en standaardisatie, waarmee aan het probleem van technische handelsbarrières een eind moest worden gemaakt. Richtlijnen volgens de "Nieuwe Aanpak" bevatten in algemene termen uiteengezette "Wezenlijke Vereisten", waaraan produkten moeten voldoen voordat ze in de EG-Lid-staten en dus ook in Nederland mogen worden verkocht. Het voldoen aan Europese Standaards zal voor handel en industrie veelal de aangewezen weg zijn om aan te tonen dat aan de wezenlijke vereisten wordt voldaan.

De richtlijnen bevatten eveneens aanwijzingen voor het aantonen van overeenstemming met de wezenlijke vereisten. Produkten die in overeenstemming zijn met de wezenlijke vereisten moeten voorzien worden van het EG-merkteken.

Op 3 mei 1989 heeft de Raad van Ministers de EMC richtlijn vastgesteld.

Het toepassingsgebied van deze richtlijn, zowel in termen van "apparaten" als in termen van "storingsfenomenen" is zeer uitgestrekt. De richtlijn heeft daarom gevolgen van een groot aantal fabrikanten, importeurs en handelaren.

De richtlijn kan niet zonder meer in de lidstaten worden toegepast doch moet eerst in de nationale wetgeving worden verwerkt. Het is de taak van de HDTP om daar zorg voor te dragen.

De richtlijn bevat geen gedetailleerde EMC-normen. De manier waarop de normen worden geformuleerd zal daarom van groot belang worden. De normen worden opgesteld door de Europese normalisatie commissies.

Wat valt er onder de richtlijn

Alle apparaten die elektromagnetische storing kunnen veroorzaken of waarvan de werking door deze storingen kan worden aangetast.

Het begrip "apparaat" moet ruim worden opgevat: "alle elektrische en elektronische apparaten alsmede uitrusting en installaties die elektrische en/of elektronische componenten bevatten". Ook het begrip "elektromagnetische storing" is ruim: "elektromagnetisch verschijnsel dat problemen in de werking van een inrichting, apparaat of systeem kan veroorzaken. Een elektromagnetische storing kan een elektromagnetische ruis, een ongewenst signaal of een wijziging in het voortplantingsmilieu zelf zijn".

Dus alle elektromagnetische fenomenen en het gehele frequentiespectrum vallen onder de richtlijn. Niet onder de richtlijn vallen apparaten die reeds onder andere richtlijnen vallen waarin EMC aspecten worden

geregeld.
Zo valt de ontsteking van motorvoertuigen onder richtlijn 72/245/EEG. Ook is er een richtlijn op komst voor sommige medische apparaten. De uitzondering omvat alleen de in deze produkt richtlijnen genoemde EMC fenomenen.
Andere fenomenen (bijvoorbeeld immuniteit van autoelektronica) zullen, zolang die niet in een andere richtlijn zijn geregeld, blijven vallen onder de EMC-richtlijn.
Ook niet onder de richtlijn valt radio-apparatuur van radio-zendamateurs behalve wanneer de apparatuur in de handel verkrijgbaar is.

De bestaande richtlijnen voor huishoudelijke apparaten/draagbaar gereedschap en fluorescentie verlichting zullen bij het in werking treden van de nieuwe richtlijn vervallen.

Beschermingseisen

Apparaten moeten aan twee beschermingseisen voldoen:

a. de opwekking van elektromagnetische storingen moet beperkt blijven tot een zodanig niveau dat radio- en telecommunicatie-apparatuur en andere apparaten overeenkomstig hun bestemming kunnen functioneren.
b. de apparaten moeten een passend niveau van intrinsieke ongevoeligheid bezitten voor elektromagnetische storingen zodat zij overeenkomstig hun bestemming kunnen functioneren.

Kortom:
Apparaten mogen andere apparaten niet storen en moeten bovendien goed blijven werken wanneer ze blootgesteld worden aan bepaalde vormen van elektrische energie.

Methoden om aan de beschermingseisen te voldoen

Fabrikanten hebben verschillende mogelijkheden om overeenstemming met de beschermingseisen aan te tonen, zij kunnen:

a. produceren overeenkomstig geharmoniseerde Europese normen, die gepubliceerd zijn door de EG en in Nederland moeten worden overgenomen;
b. indien geharmoniseerde normen ontbreken: produceren overeenkomstig nationale normen, die volgens de vereiste procedure door de Europese Commissie geaccepteerd en bekendgemaakt zijn;
c. bij het ontbreken van normen als bedoeld onder a. of b. of wanneer deze normen niet of slechts gedeeltelijk zijn toegepast de overeenstemming aantonen door middel van een technisch constructie dossier.
Dit dossier moet onder meer uiteenzetten op welke wijze de overeenstemming met de beschermingseisen is verzekerd en een technisch verslag of een certificaat bevatten van een "bevoegde instantie" (third party). Dit dossier moet gedurende 10 jaar beschikbaar blijven voor de "bevoegde autoriteiten".

Radiozendinrichtingen waarvoor typekeuring vereist is worden geacht te voldoen aan de beschermingseisen indien door een aangemelde instantie een verklaring van conformiteit is afgegeven. De EMC aspecten van telecommunicatie randapparatuur zullen naar het zich laat aanzien geregeld worden in de richtlijn voor randapparatuur die binnenkort wordt verwacht. Onder de bevoegde instantie voor het technisch verslag of certificaat wordt een keuringsinstelling verstaan die door de minister van Verkeer en Waterstaat voor deze keuringen is erkend. Aangemelde instanties voor het uitvoeren van type-keuringen moeten daarnaast ook aan de Commissie gemeld worden.

De aanduiding

In het geval de fabrikant de geharmoniseerde of erkende nationale normen toegepast heeft dient dit door middel van een EG-verklaring van overeenstemming door de fabrikant of diens gevolmachtigde te worden bevestigd. Deze verklaring dient 10 jaar beschikbaar te blijven voor de bevoegde autoriteiten. Indien noch de fabrikant noch zijn gevolmachtigde in de Gemeenschap zijn gevestigd dan rust de verplichting om de EG-verklaring van overeenstemming ter beschikking te houden bij een ieder die het apparaat op de markt brengt.
De fabrikant of diens gevolmachtigde in de Europese Gemeenschap brengt het EG-merkteken van overeenstemming aan op het apparaat of als dat niet mogelijk is op de verpakking, de gebruiksaanwijzing of het garantiebewijs.

CE

Het EG-merkteken moet voorzien zijn van het jaartal waarin het is aangebracht en in voorkomend geval worden aangevuld met de kenletters van de instelling die de EG-type verklaring heeft afgegeven. Het merkteken mag alleen gebruikt worden indien tevens aan alle andere eventueel op het apparaat van toepassing zijnde richtlijnen wordt voldaan.

Overgangsbepalingen

De richtlijn treedt in werking op 1 januari 1992 en geldt voor alle vanaf dat moment op de markt te brengen apparaten. Apparaten die op die datum al in gebruik zijn hoeven uiteraard niet aan de zelfcertificatie verplichting van de richtlijn te voldoen.
Indien Europese normen ontbreken mogen voor de betreffende produkten nationale regelgevingen tot uiterlijk 31 december 1992 worden gecontinueerd.
Deze datum staat, zoals verder op zal blijken ter discussie.

Vrij verkeer

Lid-staten moeten alle "dienstige" maatregelen nemen om ervoor te zorgen dat de apparaten alleen in de handel kunnen worden gebracht of gebruikt kunnen worden indien

zij aan de in de richtlijn gestelde eisen beantwoorden, wanneer zij op passende wijze worden geïnstalleerd en onderhouden en overeenkomstig hun bestemming worden gebruikt.
Lid-staten moeten uitgaan van het vermoeden dat apparaten die in overeenstemming zijn met een geharmoniseerde Europese norm, een geaccepteerde nationale norm of waarvoor een technisch dossier bestaat, en die voorzien zijn van een EG-merkteken, voldoen aan de beschermingseisen tenzij het tegendeel is bewezen.

Sancties

Wanneer een Lid-staat constateert dat een apparaat vergezeld van een van de genoemde certificatiemiddelen niet voldoet aan de beschermingseisen worden alle dienstige maatregelen genomen om het apparaat uit de handel te nemen, het in de handel brengen te verbieden of het vrije verkeer ervan te beperken. Lid-staten moeten ogenblikkelijk met redenen omkleed de Europese Commissie inlichten over dergelijke maatregelen.
De Commissie treedt zo snel mogelijk in overleg met betrokken partijen en zal indien de actie gerechtvaardigd wordt geacht de andere Lid-staten informeren.

Speciale maatregelen

Lid-staten mogen speciale maatregelen nemen met betrekking tot het op één bepaalde plaats in gebruik nemen en gebruiken van een apparaat, ten einde een te verwachten of bestaand probleem in verband met elektromagnetische compatibiliteit te verhelpen; speciale maatregelen mogen ook worden genomen ter bescherming van openbare telecommunicatie netten of om veiligheidsredenen gebruikte zend- of ontvangstations.
De Europese Commissie moet van dergelijke maatregelen op de hoogte worden gesteld waarna, bij erkenning door de Commissie, publikatie volgt in het publikatieblad van de EG.

Normen

De Europese Commissie heeft het Europese Elektrotechnische Normalisatie Comité CENELEC mandaat gegeven om een normenstelsel voort te brengen voor toepassing onder de EMC-richtlijn. Bestaande Europese normen worden aangepast en nieuwe ontwikkeld, doorgaans op basis van onder andere IEC en CISPR publikaties. Nederland neemt aan het CENELEC werk deel via het Nederlands Elektrotechnisch Comité (NEC), waarin de HDTP naast industrie en andere belanghebbenden participeert.

Aanpassing van de Wetgeving

De Lid-staten moeten voor 1 juli 1991 de wettelijke en bestuursrechtelijke bepalingen vaststellen en bekendmaken die nodig zijn om aan de richtlijn te voldoen. De Europese Commissie moet hiervan op de hoogte worden gesteld. In Nederland wordt elektromagnetische compatibiliteit geregeld in de Wet op de Telecommunicatievoorzieningen (WTV). Deze wet en de op de wet gebaseerde besluiten zullen worden aangepast. Een kleine werkgroep is al enige tijd bezig met het opstellen van een nieuwe EMC regelgeving.

Teneinde de richtlijn op de juiste, en in alle Lid-staten gelijke manier in te voeren onderhoudt de HDTP contact met de andere Lid-staten en de Commissie.

Knelpunten

De implementatie van de richtlijn baart nog wel enige zorgen.
In de eerste plaats betreft het de tijdige beschikbaarheid van geharmoniseerde Europese normen voor alle apparaten en EMC fenomenen die binnen de werkingssfeer van de richtlijn vallen.
De richtlijn anticipeert, gelet op de korte overgangsperiode van 1 jaar, in hoge mate op het tijdig beschikbaar zijn van deze normen.
Het ziet er naar uit dat niet alle benodigde normen, met name die voor immuniteit, op tijd beschikbaar zijn. Produkten waarvoor na 31 december 1991 geen normen beschikbaar zijn, zullen volgens de beschreven z.g.n. technische dossier route direct aan de wezenlijke vereisten getoetst moeten worden, waarbij een rapport of certificaat van een bevoegde instantie (testinstelling) nodig is. Bij massaal gebruik van deze route zal stagnatie optreden.

Doch ook produkten waarvoor, zij het in een laat stadium, wel normen beschikbaar zijn, zullen mogelijk deze technische dossier route moeten volgen. De EMC van een produkt vormt immers een integraal onderdeel van het ontwerp dat zich in een laat stadium niet even snel laat toevoegen.

Hoewel CENELEC goede vorderingen maakt, wordt ze ook gehandicapt door de uitgebreide werkingssfeer van de richtlijn, de wens om zoveel mogelijk parallel te lopen met IEC en CISPR en niet te vergeten de op het bereiken van een zo groot mogelijk consensus gebaseerde werkwijze. Een norm is en blijft ook onder de richtlijn een vrijwillig conformiteitsmiddel.

Bovendien wordt de richtlijn aangewend om normen vast te stellen voor ESD, transients en laag-frequente beïnvloeding via het lichtnet. De richtlijn werkt voor deze fenomenen als kwaliteitskatalisator.

In de tweede plaats is bij velen de vraag gerezen wat er onder de richtlijn valt en wat niet. De definitie van het begrip apparaat laat ruimte voor interpretatieverschillen. De discussie spitst zich toe op het door "derden" op de markt brengen van reserve-onderdelen, optionele printplaten voor computers en dergelijke.
Ook de essentiële vereisten voor industriële installaties en de eventuele in-situ meting van emissie en immuniteit zijn geliefde onderwerpen van discussie, evenals de vraag wanneer een produkt kan storen of gestoord kan worden en zo ja, wie dat bepaalt.

Een derde zorgenbarend aspect tenslotte is de

benodigde capaciteit aan testfaciliteiten. Het zal normaal gesproken onmogelijk zijn een EG verklaring van conformiteit op te stellen zonder dat er emissie- en immuniteitsmetingen hebben plaatsgevonden. Dit legt een zware druk op de in ons land beschikbare testcapaciteit. Veel fabrikanten beschikken over geen of onvoldoende eigen testmogelijkheden en moeten dit werk uitbesteden.
Een in de UK uitgevoerd onderzoek naar de benodigde testcapaciteit wees uit dat daar op dit moment slechts een fractie van de benodigde capaciteit voor handen is. Uiteraard hangt de omvang van dit "testknelpunt" samen met de lengte van de overgangsperiode en de interpretatie van de richtlijn m.b.t. het begrip apparaat.
Ten einde meer duidelijkheid te verkrijgen over de belangrijkste implementatie vragen is reeds begin 1990 overleg met de Commissie gestart.

Eind vorig jaar resulteerde dit in de toezegging van de Commissie een voorstel te zullen indienen om de overgangsperiode met enkele jaren te verlengen.
De richtlijn zal als dit voorstel wordt geaccepteerd gedurende deze periode optioneel zijn hetgeen wil zeggen dat apparaten die conform de richtlijn op de markt worden gebracht geen handelsbarrieres in Europa mogen ontmoeten.
Daarnaast kan volgens de nationale regelingen worden geproduceerd, doch een vrij verkeer van goederen is dan niet gegarandeerd.
De Commissie zegde voorts toe te zullen komen met een informatief document over het begrip "op de markt brengen" en met een informatief document inzake de definitie van het begrip "apparaat".

Conclusies

De EMC-richtlijn heeft consequentie voor grote sectoren van handel en industrie.
Het moeten voldoen aan de wezenlijke vereisten zal het toepasen van geharmoniseerde normen sterk bevorderen.
Dan moeten er natuurlijk wel normen zijn.
Want het alternatief, het volgen van de technische dossier route, lijkt omslachtig, tijdrovend en kostbaar.
Het is zeer de vraag of de benodigde normen tijdig beschikbaar zijn. Onder meer om deze reden hebben de Lid-staten aangedrongen op een langere overgangstermijn.
Het is uiteraard niet de bedoeling het handel en industrie alleen maar lastig te maken.
Implementatie van de EMC-richtlijn betekent voor hen vooral een gegarandeerd vrij verkeer van goederen binnen Europa, voor wat betreft EMC.
Voor de eindgebruiker tenslotte betekent de richtlijn meer zekerheid op het gebied van EMC.

Voordracht gehouden tijdens de 384e werkvergadering.

VEDERPRIJS 1988

Tijdens de 383e werkvergadering, welke op 6 november 1990 gehouden werd in het Nationaal Lucht en Ruimtevaart Laboratorium in de Noordoostpolder, werd de Vederprijs 1988 uitgereikt door Mevrouw E.J. Kosters-van Hoboken, kleindochter van de Heer A. Veder, aan



DR.IR. R.J. VAN DE PLASSCHE.

De considerans, welke werd uitgesproken door Prof.Ir. A. Kok, is onderstaand afgedrukt.

Het NERG en het WERA-fonds VEDER hebben een parallel in hun doelstelling, die in de trefwoordcombinatie "Radio-elektronica" tot uitdrukking kan worden gebracht, en dat dan opgevat in de meest ruime zin. Het is dan ook min of meer tot traditie geworden om de VEDER-prijsuitreiking in een werkvergadering van het NERG te laten plaatsvinden. Het bestuur van het VEDER-fonds dankt de verenigingen, die deze werkvergadering hebben belegd, voor de geboden gelegenheid om ook vandaag aandacht te besteden aan de toekenning van de VEDER-prijs 1988.

Het veld van de elektronische radiotechniek, en meer in het algemeen de communicatietechniek, wordt in zijn hedendaagse ontwikkeling gedreven, enerzijds door de digitalisering van informatie-overdracht en -verwerking, een ontwikkeling die al enkele tientallen jaren aan de gang is, maar nog steeds een stempel drukt op de hedendaagse ontwikkelingen; anderzijds en wat recenter door de opkomst van optische technologieën, zich uitend in optische transmissie via fibers en de ontwikkeling van modulatie- en multiplexsystemen van ongekend hoge capaciteiten en de ontwikkeling van nieuwe optische componenten voor de verwerking en sturing van deze informatiestromen in netwerken. Als resultaat van deze geweldig interessante ontwikkelingen kan ons in vergaderingen als deze telkens weer verslag worden uitgebracht over nieuwe ontwikkelingen in transmissiesystemen, schakelprincipes, LAN's, MAN's, WAN's en andere netwerken en systemen en daardoor gedragen nieuwe applicaties.

Daarbij dreigen ontwikkelingen van subsystemen en sub-subsystemen en ontwikkelingen op component-niveau wat onderbelicht te raken.

Eén van deze gebieden betreft de A/D- en de D/A-conversie, een gebied dat toch een sleutelrol vervult als het erom gaat om signalen uit de fysische wereld toegang te geven tot onze digitale wereld van signaaltransport en signaalverwerking en zonodig weer te representeren in een fysische verschijningsvorm. Het is o.a. de taak van programmacommissies van betreffende verenigingen om te zorgen dat ook dergelijke gebieden onder de publieke aandacht komen. Ditmaal is de VEDER-prijs in het veld van A/D-conversie terechtgekomen en wel door beloning van het werk van Ir. R.J. Van de Plassche, die veel en zeer verdienstelijk werk heeft verricht op het gebied van de A/D- en D/A-conversie, en inmiddels op grond van dit werk de graad van doctor in de technische wetenschappen heeft behaald.

Van de Plassche heeft op dit terrein baanbrekend werk verricht van een hoog innovatief gehalte. Niet alleen heeft hij zich een zeer goede algemene kennis omtrent de problematiek bij A/D- en D/A-conversie eigen gemaakt; hij heeft ook in sterke mate bijgedragen tot de oplossing van onderkende bottlenecks en hij heeft daarbij een zeer grote mate van nauwkeurigheid weten te realiseren in geïntegreerde circuits ondanks de door de integratie-technologie bepaalde beperkingen. Daarbij is te bedenken dat de nauwkeurigheid ons hier niet door een gunstige speling van het natuurlijke lot in de schoot wordt geworpen. Denk bijvoorbeeld aan de relatieve tijdnauwkeurigheid van 1 op 10^6, waarmee een eenvoudig kristalletje onze horloges van de juiste tijd voorziet; om maar niet te spreken van de nauwkeurigheid van atoomklokken. Nee, bij A/D- en D/A-convertors moet men eerder denken aan natuurlijke nauwkeurigheden die in de orde van 0,1% liggen en waarbij elke ordeverbetering door listigheid en zorgvuldigheid moet worden bevochten.

Het is misschien goed om hier als voorbeeld even enkele tot de verbeelding sprekende punten te noemen, die men bij hoge kwaliteit audio A/D-conversie ontmoet.

- Een 16 bits A/D-convertor met zeer hoogwaardige dynamische respons vereist een stopbandonderdrukking van de orde van 120 dB d.i. een vermogensdiscriminatiefactor van 10^{12}.
- Eenzelfde convertor vereist een nauwkeurigheid in de bemonsterings-timing van beter dan 1/4 nsec.
- Het eindresultaat moet in amplitude nauwkeuriger zijn dan 1 op 2^{17}, d.i. 1 op 10^5.
- Omgezet in absolute nauwkeurigheid moet deze over alle 65.000 niveaus gelden en over een groot temperatuurbereik.
- Een zeer belangrijk punt is ook het dynamische gedrag van de schakeling en de ruis en besturingsoverspraak, waaraan zeer hoge eisen worden gesteld.
- Ook is het geen sinecure om produkten van een dergelijk hoge prestatiegraad op de juiste wijze te verifiëren op hun geclaimde eigenschappen.

Het is aan het realiseren en opschroeven van prestaties van deze soort in de techniek dat Van de Plassche gedurende een groot aantal jaren zijn bijdragen heeft geleverd, zowel aan audio als aan videoconvertors, vooral ook aan realiseringen daarvan in monolithische circuits.

Daarnaast herkende het bestuur ook nog andere creatieve werkzaamheden op het gebied van de integreerbare analoge signaalverwerkingstechniek.

Hoewel het bestuur beseft dat velen naast hem aan deze materie hebben gewerkt heeft het bestuur gemeend Van de Plassche te moeten eren met de VEDER-prijs 1988 wegens de op dat moment herkenbare beste Nederlandse prestaties op dit gebied.

Ik wens hem daarmee van harte geluk en wil dan nu gaarne plaats maken voor mevrouw Kosters, voorzitter van het WERA-fonds VEDER voor de feitelijke prijsuitreiking.

UIT HET NERG

LEDENMUTATIES

Voorgestelde leden

Ir. J.C. Buisman, Vechtstraat 58, 1823 VB ALKMAAR.
J.H.P. Diederen, Vestdijk 37-K, 5611 CA EINDHOVEN.
Ir. A.W. Doorduin, Oosterend 4 A, 1251 HN LAREN.
J.C. van Essen, Teylingerlaan 45, 2171 CC SASSENHEIM.
Ir. R. Hekmat, Korvezeestraat 266, 2628 DM DELFT.
Mw. MA J.M. Scarr, Herenwaard 23, 2716 XR ZOETERMEER.
Ing. B. Schipper, Marga Klompéstraat 8,
2401 ME ALPHEN A/D RIJN.
Ir. P.C.W. Sommen, p/a Technische Universiteit Eindhoven,
Faculteit Elektrotechniek, Gebouw EH 9.07, Postbus 513,
5600 MB EINDHOVEN.
Ir. C.P. Spruijt, Schenkkade 231 A, 2595 AV DEN HAAG.

Nieuwe leden

Ir. E. Bobeldijk, Boeninlaan 59, 1102 TH AMSTERDAM.
Ir. E. Drijver, Levendaal 86, 2311 JN LEIDEN.
Mw. ir. T.L. Hamann, Nederlandplein 10, 5628 AD EINDHOVEN.
Ir. J.J. Jacobs, Van Alkemadelaan 61, 2697 AB DEN HAAG.
Ir. A.J. van Rhijn, Korvezeestraat 426, 2628 DV DELFT
Ir. F.J. Sluijs, Mensinge 11, 5655 HT EINDHOVEN.
Ir. R.M. Wiegers, Bergse Plaslaan 2, 3054 AR ROTTERDAM.

Nieuwe adressen van leden

Ir. A. Bakker, Terlindenweg 22, 6433 PC HOENSBROEK.
Prof. dr. ir. G. Brussaard, Jeroen Boschlaan 205,
5642 AS EINDHOVEN.
A.P.K. Elhorst, Witte Heerenstraat 8, 2011 NV HAARLEM.
Ir. F.W. Greuter, Mr. P.J. Troelstrastraat 8, 7556 EM HENGELO.
Prof. dr. ing. J.A.G. Jess, Loondermolen 52, 5612 MG EINDHOVEN.
C. Joosse, Aaldert 12, 6617 AL BERGHAREN (Gld.)
Ir. W. Jouwsma, Vordensebinnenweg 1, 7241 RM LOCHEM.
H.J. Kip, Lariksstraat 4, 7132 CS LICHTENVOORDE.
J.C. Leguijt, Postbus 1178, 1270 BD HUIZEN.
Ir. F. Möhring, Elsmansdijk 1, 7161 NA NEEDE.
Ir. G. Radstake, Hoofdstraat 59, 7981 AD DIEVER.
Ir. J. van Rees, Ieplaan 14, 2541 BT LEIMUIDEN.
Prof. dr. ir. E. Seevinck, Philips' Nat. Lab., Gebouw WAY-2,
Postbus 80000, 5600 JA EINDHOVEN.
Drs. P.F.J. van Velthoven, Beatrixpark 33, 4872 BH ETTEN-LEUR.
Ing. G.J. van Velzen, Frederikslaan 8, 2182 DD HILLEGOM.
Dr. ir. A.J. Vinck, Inst. für Experimentelle Mathematik,
Ellerstr. 29, ESSEN, Duitsland.
P. de Waard, Burg. Wouterslaan 8, 2681 CZ MONSTER.
H. van der Weijden, Belgiëpark 18, 2408 CS ALPHEN A/D RIJN.

Concept programma NERG 1991

WV 386+
26 maart
AES
Digital Editing
Veenendaal

JV & WV 387
10 april
Van radiotechniek tot ULSI
TU Delft

WV 388+
26 april
AES
Kortegolf Wereldomroep
?

WV 389+
5 juni
IEEE
Supergeleiding
?

WV 390+
12 juni
Micro-elektronische Sensoren
Eindhoven

WV 391+
September
WARC Frequentie allocatie
?

Suggesties voor '92: Neurale systemen, Bezoek Telematica Lab.

WV = werkvergadering, uitsluitend voor NERG-leden;
WV+ = werkvergadering, voor NERG-, AES- en IEEE-leden;
WB = werkbezoek, uitsluitend voor NERG-leden;
JV = jaarvergadering, uitsluitend voor NERG-leden;
SMR = semiminar.

Tijdschrift van het Nederlands Elektronica- en Radiogenootschap

Inhoud

deel 56 – nr. 1 – 1991

Druk: de Witte, Eindhoven.